



## BR-6215NRg

### NAS Broadband Router



## *User's Manual*



Copyright© by Edimax Technology Co, LTD. all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this Company

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes

The product you have purchased and the setup screen may appear slightly different from those shown in this QIG. For more detailed information about this product, please refer to the User's Manual on the CD-ROM. The software and specifications subject to change without notice. Please visit our web site [www.edimax.com.tw](http://www.edimax.com.tw) for the update. All right reserved including all brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders

#### Linux Open Source Code

Certain Edimax products include software code developed by third parties, including software code subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL"). Please see the **GNU** ([www.gnu.org](http://www.gnu.org)) and **LPGL** ([www.gnu.org](http://www.gnu.org)) Web sites to view the terms of each license.

The GPL Code and LGPL Code used in Edimax products are distributed without any warranty and are subject to the copyrights of their authors. For details, see the GPL Code and LGPL Code licenses. You can download the firmware-files at <http://www.edimax.com.tw> under "Download" page.

- ※ The product you have purchased and the setup screen may appear slightly different from those shown in this QIG. For more detailed information about this product, please refer to the User's Manual on the CD-ROM.
- ※ Software and specifications subject to change without notice. Please visit our web site for the update.
- ※ All rights reserved. Trademarks or registered trademarks are the property of their respective holders

Introduction .....	4
Features .....	4
Minimum Requirements .....	4
Package Content .....	4
Note .....	4
Get to know the Broadband Router .....	4
Back Panel .....	4
Front Panel .....	5
Setup Diagram .....	6
Getting started .....	6
Chapter 1 .....	10
Quick Setup .....	10
Step 1) Time Zone .....	10
Step 2) Broadband Type .....	11
1.1 Cable Modem .....	11
1.2 Fixed-IP xDSL .....	12
1.3 PPPoE .....	14
1.4 PPTP .....	15
1.5 L2TP .....	16
1.6 Telstra Big Pond .....	18
Chapter 2 .....	19
General Settings .....	19
2.1 System .....	20
2.1.1 Time Zone .....	20
2.1.2 Password Settings .....	21
2.1.3 Remote Management .....	21
2.2 WAN .....	22
2.2.1 Dynamic IP .....	24
2.2.2 Static IP Address .....	24
2.2.3 PPPoE (PPP over Ethernet) .....	24
2.2.4 PPTP .....	24
2.2.5 L2TP .....	24
2.2.6 Telstra Big Pond .....	24
2.2.7 DNS .....	24
2.2.8 DDNS .....	26
2.3 LAN .....	26
2.4 Wireless .....	28
2.4.1 Basic Settings .....	29
2.4.2 Advanced Settings .....	30
2.4.3 Security .....	31
2.4.3.1 WEP only .....	31
2.4.3.2 802.1x only .....	33
2.4.3.3 802.1x WEP Static key .....	33
2.4.3.4 WPA Pre-shared key .....	35
2.4.3.5 WPA Radius .....	35
2.4.4 Access Control .....	36
2.6 NAT .....	40
2.6.1 Port Forwarding .....	40
2.6.2 Virtual Server .....	41
2.6.3 Special Applications .....	43
2.6.4 UPnP Settings .....	44
2.6.5 ALG Settings .....	45
2.6.6 Static Routing .....	45
2.7 Firewall .....	46
2.7.1 Access Control .....	47
2.7.2 URL Blocking .....	49
2.7.3 DoS (Denial of Service) .....	50
2.7.4 DMZ .....	51
2.8 Print Server .....	51
2.8.1 LPR Printing .....	52
2.8.2 IPP Printing .....	56
2.9 File/FTP Server .....	59
2.9.1 Users setup .....	60

Add a New User .....	60
2.9.2 File Server setup.....	61
Add/Edit Shared Folder .....	62
Open Dialog.....	63
2.9.3 FTP Server.....	63
Add/Edit FTP Folder .....	64
Open Dialog.....	64
2.9.4 Storage Tool.....	65
Auto Partition & Formatting .....	66
Add Partition .....	66
2.9.5 Storage Status .....	67
Chapter 3 .....	68
Status .....	68
3.1 Status and Information .....	68
3.2 Internet Connection.....	69
3.3 Device Status .....	69
3.4 System Log .....	71
3.5 Security Log.....	71
3.6 Active DHCP Client.....	72
3.7 Statistics.....	72
Chapter 4 .....	73
Tool .....	73
4.1 Configuration Tools.....	73
4.2 Firmware Upgrade .....	75
4.3 Reset .....	75
Appendix A.....	77
Glossary .....	78

## Introduction

Congratulations on purchasing this Wireless Broadband Router. This Wireless Broadband Router is a cost-effective IP Sharing Router with NAS and print server supported that enables multiple users to share the Internet, files and printer through an ADSL or cable modem. Simply configure your Internet connection settings in the Wireless Broadband Router and plug your PC to the LAN port and you're ready to share files and access the Internet. As your network grows, you can connect another hub or switch to the router's LAN ports, allowing you to easily expand your network. The Wireless Broadband Router is embedded with an IEEE 802.11g/b access point that allows you to build up a wireless LAN. The Wireless Broadband Router provides a total solution for the Small and Medium-sized Business (SMB) and the Small Office/Home Office (SOHO) markets, giving you an instant network today, and the flexibility to handle tomorrow's expansion and speed.

## Features

- High Internet Access throughput (up to 50M)
- Allow multiple users to share a single Internet line
- Supports up to 253 networking client users
- Provides two USB port for connecting with USB printer or USB mass storage devices
- Internet Access via Cable or xDSL modem
- Allow you to share your files via FTP or Network Neighborhood
- Access Private LAN Servers from the Public Network
- Equipped with four LAN ports (10/100M) and one WAN port (10/100M)
- Provides IEEE 802.11g/b wireless LAN access point
- Support DHCP (Server/Client) for easy setup
- Support advance features such as: Special Applications, DMZ, Virtual Servers, Access Control, Firewall
- Allow you to monitor the router's status such as: DHCP Client Log, System Log, Security Log and Device/Connection Status
- Easy to use Web-based GUI for configuration and management
- Remote Management allows configuration and upgrades from a remote site (over the Internet)

## Minimum Requirements

- One External xDSL (ADSL) or Cable modem with an Ethernet port (RJ-45)
- Network Interface Card (NIC) for each Personal Computer (PC)
- PCs with a Web-Browser (Internet Explorer 5.0 or higher, or Netscape Navigator 7.2 or higher)

## Package Content

- One Wireless Broadband Router / One Quick Installation Guide
- One User Manual CD / One Power Adapter / Other Accessories

## Note

The WAN "idle timeout" auto-disconnect function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly when you use this function in the first time, especially your ISP charge you by time used.

## Get to know the Broadband Router

### Back Panel

The diagram (fig1.0) below shows the broadband router's back panel. The router's back panel is divided into four sections, **LAN**, **WAN**, **USB**, and **Reset**:

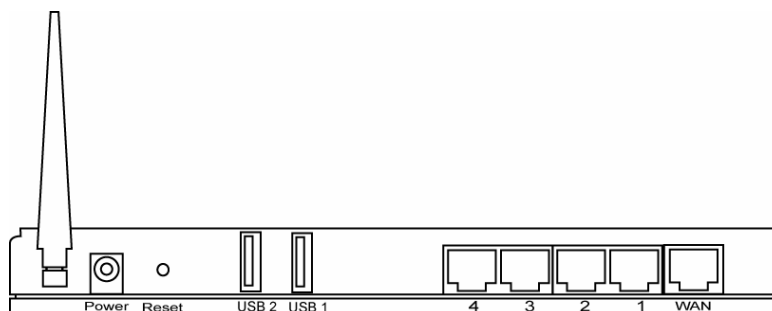


Figure 1.0

### 1) Local Area Network (LAN)

The Broadband router's 4 LAN ports are where you connect your LAN's PCs, printer servers, hubs and switches etc.

### 2) Wide Area Network (WAN)

The WAN port is the segment connected to your xDSL or Cable modem and is linked to the Internet.

### 3) USB

The USB ports allow you to share your files or printer through them. Each port can support both printer and USB mass storage devices.

**Note 1: Please plug the external power to your USB mass storage devices.**

**Note 2: Please plug the USB mass storage dedicated to this NAS router in the USB 1 port for better management function and plug the USB flash disk used to share files among different PCs and notebooks in the USB 2 port for instant setup.**

### 4) Reset

The Reset button allows you to:

- 1) If problems persist or you experience extreme problems or you forgot your password, press the reset button for **longer** than 5 seconds and the router will reset itself to the factory default settings (**warning**: your original configurations will be replaced with the factory default settings)

### Front Panel

On the router's front panel there are LED lights that inform you of the router's current status. Below is an explanation of each LED and its description.

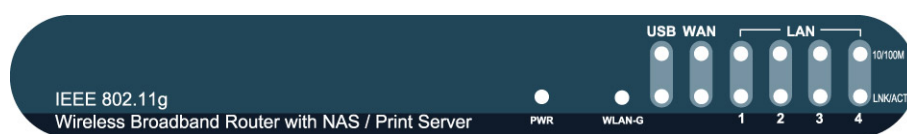


Figure 1.1

LED	Light Status	Description
PWR	ON	Router's power supply is on
WAN 10/100M	ON	WAN port 100Mbps is connected
	Off	WAN port 10Mbps is connected
WAN LNK/ACT	ON	WAN is connected
	Off	No WAN connection
	Flashing	WAN port is Activity (ACT)
LAN 10/100M (Port 1-4)	ON	LAN port 100Mbps is connected
	Off	LAN port 10Mbps is connected
LAN LNK/ACT (Port 1-4)	ON	LAN is connected
	Off	No LAN connection
	Flashing	LAN port is Activity (ACT)
USB	ON	USB storage device is connected
	Off	No USB storage device connection
	Flashing	USB printer is printing. (ACT)
WLAN-G	ON	Wireless LAN has been activated
	Off	Wireless LAN is disabled
	Flashing	Wireless LAN is Activity (ACT)

## Setup Diagram

Figure 1.2 below shows a typical setup for a Local Area Network (LAN).

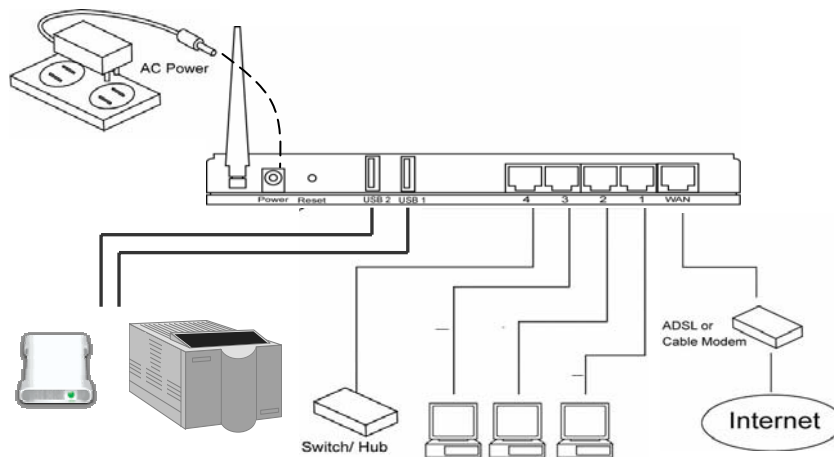


Figure 1.2

## Getting started

This is a step-by-step instruction on how to start using the router and get connected to the Internet.

1) Setup your network as shown in the setup diagram above (fig 1.2).

2) You then need to set your LAN PC clients so that it can obtain an IP address automatically. All LAN clients require an IP address. Just like an address, it allows LAN clients to find one another. (If you have already configured your PC to obtain an IP automatically then proceed to step 3, page 11)

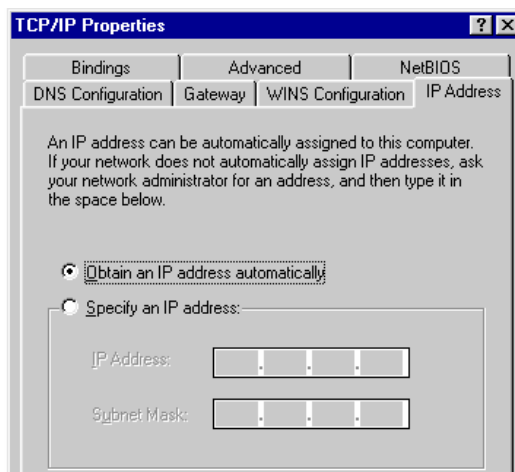
### Configure your PC to obtain an IP address automatically

By default the broadband router's DHCP is on, this means that you can obtain an IP address automatically once you've configured your PC to obtain an IP address automatically. This section will show you how to configure your PC's so that it can obtain an IP address automatically for either Windows 95/98/Me, 2000 or NT operating systems. For other operating systems (Macintosh, Sun, etc.), follow the manufacturer's instructions. The following is a step-by-step illustration on how to configure your PC to obtain an IP address automatically for 2a) **Windows 95/98/Me**, 2b) **Windows XP**, 2c) **Windows 2000** and 2d) **Windows NT**.

#### 2a) Windows 95/98/Me

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
2. Double-click *Network* icon. The *Network* window will appear.
3. Check your list of Network Components. If TCP/IP is not installed, click the *Add* button to install it. If TCP/IP is installed, go to **step 6**.
4. In the *Network Component Type* dialog box, select *Protocol* and click *Add* button.
5. In the *Select Network Protocol* dialog box, select *Microsoft* and *TCP/IP* and then click the *OK* button to start installing the TCP/IP protocol. You may need your Windows CD to complete the installation.
6. After installing TCP/IP, go back to the Network dialog box. Select TCP/IP from the list of Network Components and then click the Properties button.
7. Check each of the tabs and verify the following settings:

- **Bindings:** Check *Client for Microsoft Networks* and *File and printer sharing for Microsoft Networks*.
- **Gateway:** All fields are blank.
- **DNS Configuration:** Select *Disable DNS*.
- **WINS Configuration:** Select *Disable WINS Resolution*.
- **IP Address:** Select *Obtain IP address automatically*.

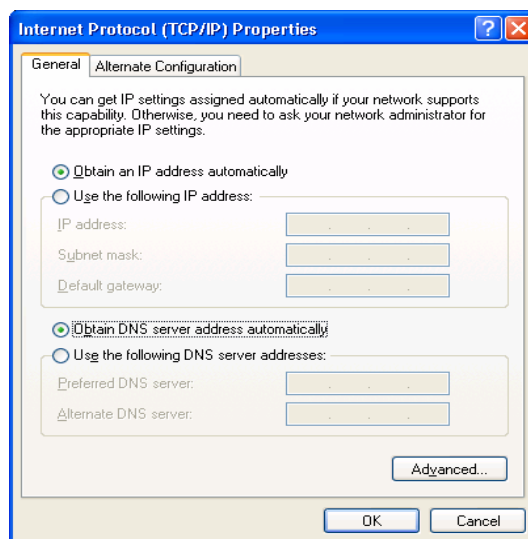


8. Reboot the PC. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

**Note:** Please make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN. Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3

## 2b) Windows XP

1. Click the *Start* button and select *Settings*, then click *Network Connections*. The *Network Connections* window will appear.
2. Double-click *Local Area Connection* icon. The *Local Area Connection* window will appear.
3. Check your list of Network Components. You should see *Internet Protocol [TCP/IP]* on your list. Select it and click the *Properties* button.
4. In the Internet Protocol (TCP/IP) Properties window, select *Obtain an IP address automatically* and *Obtain DNS server address automatically* as shown on the following screen.



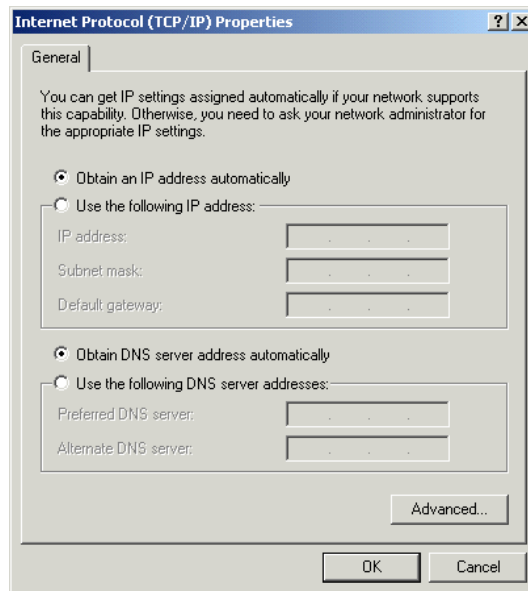
5. Click *OK* to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

**Note:** Please make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN. Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3

## 2c) Windows 2000

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
2. Double-click *Network and Dial-up Connections* icon. In the *Network and Dial-up Connection* window, double-click *Local Area Connection* icon. The *Local Area Connection* window will appear.
3. In the *Local Area Connection* window, click the *Properties* button.
4. Check your list of Network Components. You should see *Internet Protocol [TCP/IP]* on your list. Select it and click the *Properties* button.
5. In the Internet Protocol (TCP/IP) Properties window, select *Obtain an IP address automatically* and *Obtain DNS server address automatically* as shown on the following screen.



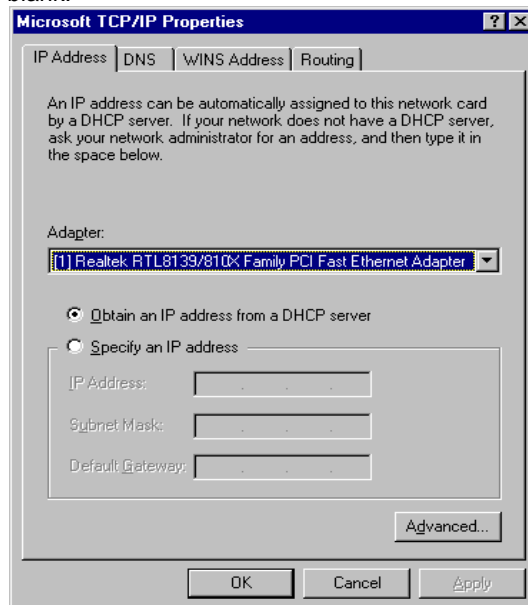


6. Click **OK** to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

**Note:** Please make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN. Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3.

## 2d) Windows NT

1. Click the **Start** button and select **Settings**, then click **Control Panel**. The **Control Panel** window will appear.
2. Double-click **Network** icon. The **Network** window will appear. Select the **Protocol** tab from the **Network** window.
3. Check if the **TCP/IP Protocol** is on your list of **Network Protocols**. If TCP/IP is not installed, click the **Add** button to install it now. If TCP/IP is installed, go to **step 5**.
4. In the **Select Network Protocol** window, select the **TCP/IP Protocol** and click the **Ok** button to start installing the TCP/IP protocol. You may need your Windows CD to complete the installation.
5. After you install TCP/IP, go back to the **Network** window. Select TCP/IP from the list of **Network Protocols** and then click the **Properties** button.
6. Check each of the tabs and verify the following settings:
  - **IP Address:** Select *Obtain an IP address from a DHCP server*.
  - **DNS:** Let all fields be blank.
  - **WINS:** Let all fields be blank.
  - **Routing:** Let all fields be blank.



7. Click **OK** to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

**Note:** Please make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN. Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3.

3) Once you have configured your PCs to obtain an IP address automatically, the router's DHCP server will automatically give your LAN clients an IP address. By default the Broadband Router's DHCP server is enabled so that you can obtain an IP address automatically. To see if you have obtained an IP address, see Appendix A.

**Note:** Please make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN. If there is another DHCP on your network, then you'll need to switch one of the DHCP servers off. (To disable the Broadband router's DHCP server see chapter 2 LAN Port)

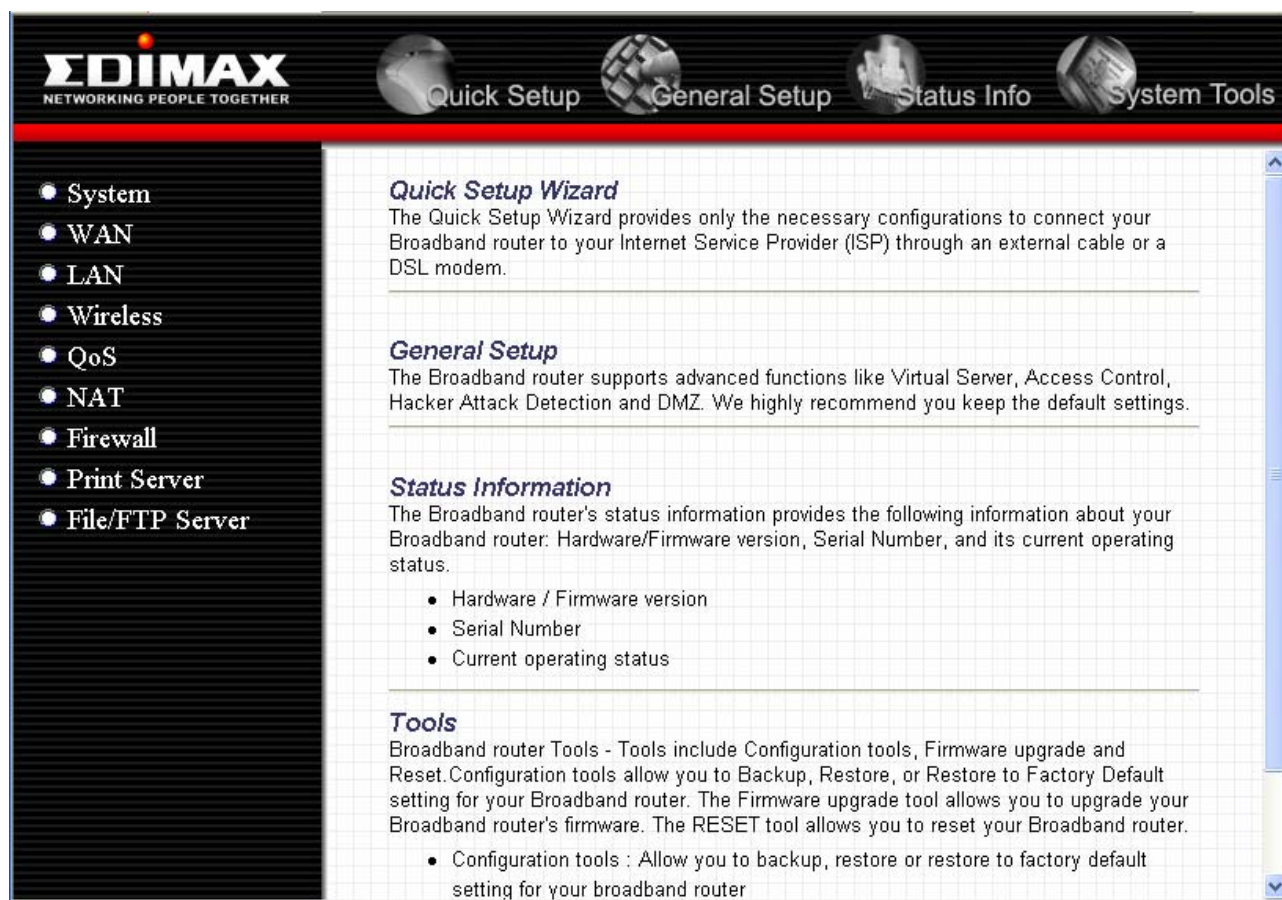
4) Once your PC has obtained an IP address from your router, enter the default IP address **192.168.2.1** (broadband router's IP address) into your PC's web browser and press <enter>

5) The login screen below will appear. Enter the "User Name" and "Password" and then click <OK> to login.

**Note:** By default the user name is "admin" and the password is "1234". For security reasons it is recommended that you change the password as soon as possible (in General setup/system/password, see chapter 2)



6) The **HOME** page screen below will appear. The **Home** Page is divided into four sections, **Quick Setup Wizard**, **General Setup**, **Status Info** and **System Tools**.



**Quick Setup Wizard (Chapter 1)**

Select your Internet connection type and then input the configurations needed to connect to your Internet Service Provider (ISP).

### General Setup (Chapter 2)

This section contains configurations for the Broadband router's advance functions such as: Address Mapping, Virtual Server, Access Control, Hacker Attack Prevention, DMZ, Special applications and other functions to meet your LAN requirements.

### Status Info (Chapter 3)

In this section you can see the Broadband router's system information, Internet Connection, Device Status, System Log, Security Log and DHCP client information.

### Tools (Chapter 4)

This section contains the broadband router's Tools - Tools include Configuration tools, Firmware upgrade and Reset. Configuration tools allow you to Backup (save), Restore, or Restore to Factory Default configuration for your Broadband router. The Firmware upgrade tool allows you to upgrade your Broadband router's firmware. The RESET tool allows you to reset your Broadband router.

- 7) Click on **Quick Setup Wizard** (see chapter 1) to start configuring settings required by your ISP so that you can start accessing the Internet. The other sections (General Setup, Status Information and Tools) do not need to be configured unless you wish to implement/monitor more advance features/information.  
Select the section (Quick Setup Wizard, General Setup, Status Information and Tools) you wish to configure and proceed to the corresponding chapter.

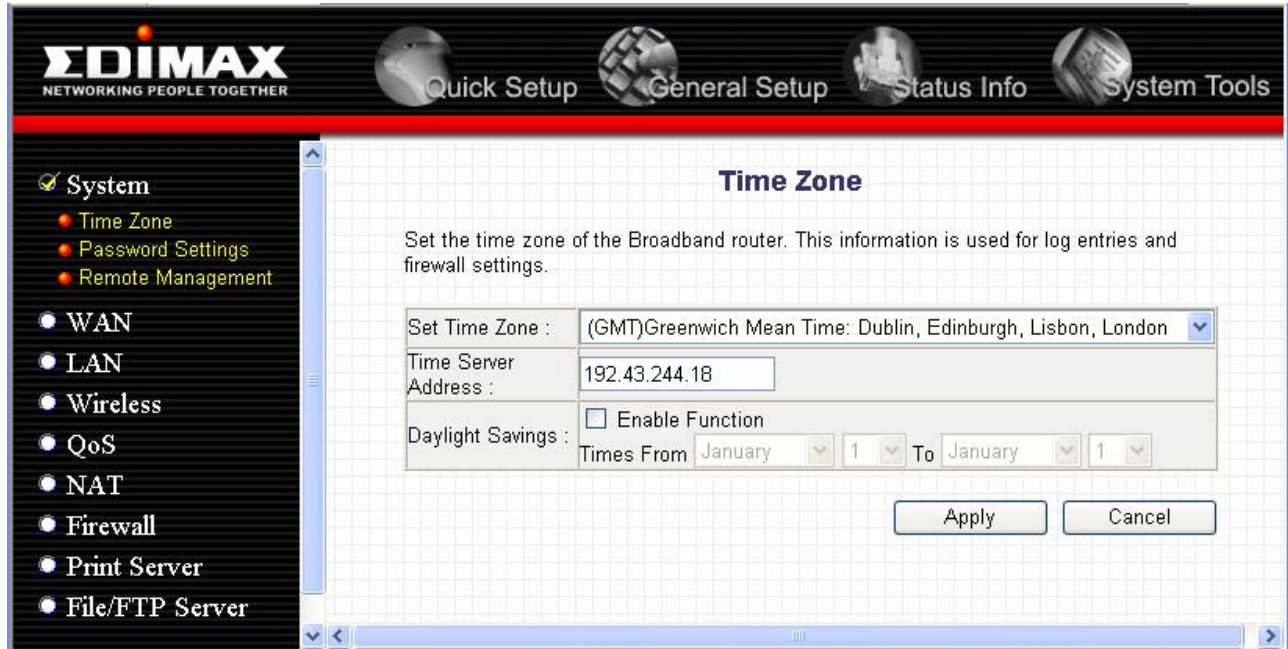
## Chapter 1

### Quick Setup

The Quick Setup section is designed to get you using the broadband router as quickly as possible. In the Quick Setup you are required to fill in only the information necessary to access the Internet. Once you click on the **Quick Setup Wizard** in the HOME page, you should see the screen below.

#### Step 1) Time Zone

The Time Zone allows your router to base its time on the settings configured here, this will affect functions such as Log entries and Firewall settings.



Parameter	Description
Set Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection
Time Server Address	You can manually assign time server address if the default time server dose not work
Daylight Savings	The router can also take Daylight savings into account. If you wish to use this function, you must check/tick the enable box to enable your daylight saving configuration (below)
Times From	Select the period in which you wish to start daylight Savings Time

Times to	Select the period in which you wish to end daylight Savings Time
----------	--

Click on **NEXT** to proceed to the next page (step 2) Broadband Type.

## Step 2) Broadband Type

In this section you have to select one of four types of connections that you will be using to connect your broadband router's WAN port to your ISP (see screen below).

**Note:** Different ISP's require different methods of connecting to the Internet, please check with your ISP as to the type of connection it requires.

Menu	Description
Cable Modem	Your ISP will automatically give you an IP address
Fixed-IP xDSL	Your ISP has given you an IP address already
PPPoE xDSL	Your ISP requires you to use a Point-to-Point Protocol over Ethernet (PPPoE) connection.
PPTP xDSL	Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection.
L2TP xDSL	Your ISP requires you to use a Layer Two Tunneling Protocol (L2TP) connection.
Telstra Big Pond	This Protocol only used for Australia's ISP connection.


Click on one of the WAN type and then proceed to the manual's relevant sub-section (**1.1**, **1.2**, **1.3**, **1.4**, **1.5** or **1.6**). Click on **Back** to return to the previous screen.

### 1.1 Cable Modem

Choose Cable Modem if your ISP will automatically give you an IP address. Some ISP's may also require that you fill in additional information such as Host Name and MAC address (see screen below).

**Note:** The Host Name and MAC address section is *optional* and you can skip this section if your ISP does not require these settings for you to connect to the Internet.





Quick Setup
General Setup
Status Info
System Tools

1. Time Zone

2. Broadband Type

3. IP Address Info

### Cable Modem


Host Name	<input type="text"/>
MAC address	<input type="text" value="000000000000"/>
<input type="button" value="Clone Mac address"/>	
TTL :	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled

Parameters	Description
Host Name	If your ISP requires a Host Name, type in the host name provided by your ISP, otherwise leave it blank if your ISP does not require a Host Name.
MAC Address	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this MAC address in this section or use the " <b>Clone MAC Address</b> " button to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work). To find out the PC's MAC address see Appendix A. (see Glossary for an explanation on MAC address)

Click <OK> when you have finished the configuration above. **Congratulations!** You have completed the configuration for the Cable Modem connection. You can start using the router now, if you wish to use some of the advance features supported by this router see chapter 2, 3, 4.

## 1.2 Fixed-IP xDSL

Select Static-IP xDSL if your ISP has given you a specific IP address for you to use. Your ISP should provide all the information required in this section.



Quick Setup
General Setup
Status Info
System Tools

1. Time Zone

2. Broadband Type

3. IP Address Info

### Fixed-IP xDSL

Enter the IP Address, Subnet Mask, Gateway IP Address and DNS IP Address provided to you by your ISP in the appropriate fields.

IP address assigned by your Service Provider	<input type="text" value="172.1.1.1"/>
Subnet Mask	<input type="text" value="255.255.0.0"/>
DNS address	<input type="text"/>
Service Provider Gateway Address	<input type="text" value="172.1.1.254"/>
TTL :	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled

Parameters	Description
IP address	This is the IP address that your ISP has given you.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0)
Gateway address	This is the ISP's IP address gateway

Click <**OK**> when you have finished the configuration above. **Congratulations!** You have completed the configuration for the Static-IP x DSL connection. You can start using the router now, if you wish to use some of the advance features supported by this router see chapter 2, 3, 4.

### 1.3 PPPoE

Select PPPoE if your ISP requires the PPPoE protocol to connect you to the Internet. Your ISP should provide all the information required in this section.

The screenshot shows the EDIMAX router configuration web interface. The top navigation bar includes links for Quick Setup, General Setup, Status Info, and System Tools. On the left sidebar, there are three menu items: 1. Time Zone, 2. Broadband Type, and 3. IP Address Info. The main content area is titled 'PPPoE' and contains instructions: 'Enter the User Name and Password required by your ISP in the appropriate fields. If your ISP has provided you with a "Service Name" enter it in the Service Name field, otherwise, leave it blank.' Below the instructions is a form titled 'Use PPPoE Authentication' with the following fields: User Name, Password, Service Name, MTU (set to 1392, with a note '(512<=MTU Value<=1492)'), Connection Type (set to Continuous, with buttons for Connect and Disconnect), Idle Time Out (set to 10, with a note '(1-1000 minutes)'), and TTL (with radio buttons for Disabled and Enabled). At the bottom right of the form are 'Back' and 'OK' buttons.

Parameter	Description
User Name	Enter the User Name provided by your ISP for the PPPoE connection
Password	Enter the Password provided by your ISP for the PPPoE connection
Service Name	This is optional. Enter the Service name should your ISP requires it, otherwise leave it blank.
MTU	This is optional. You can specify the maximum size of your transmission packet to the Internet. Leave it as it is if you to not wish to set a maximum packet size.
Connection Type	<p>If you select "Continuous", the router will always connect to the ISP. If the WAN line breaks down and links again, the router will auto-reconnect to the ISP.</p> <p>If you select "Connect On Demand", the router will auto-connect to the ISP when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "Idle Time".</p> <p>If you select "Manual", the router will connect to ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not disconnect due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP.</p>
Idle Time	<p>You can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent (no one using the Internet) during this specified period, the router will automatically disconnect the connection with your ISP.</p> <p><b>Note:</b> This "idle timeout" function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly when you use this function in the first time, especially your ISP charge you by time used.</p>

Click <OK> when you have finished the configuration above. **Congratulations!** You have completed the configuration for the PPPoE connection. You can start using the router now, if you wish to use some of the advance features supported by this router see chapter 2, 3, 4.

## 1.4 PPTP

Select PPTP if your ISP requires the PPTP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.

**PPTP**  
 Point-to-Point Tunneling Protocol is a common connection method used in xDSL connections.

**WAN Interface Settings**

☒ **Obtain an IP address automatically**

Host Name   
 MAC address

☐ **Use the following IP address**

IP address   
 Subnet Mask   
 Default Gateway

**PPTP Settings**

User ID   
 Password   
 PPTP Gateway   
 Connection ID  (Optional)  
 MTU  (512<= MTU Value<=1492)  
 BEZEQ-ISRAEL ☐ Enable (for BEZEQ network in ISRAEL use only)  
 Connection Type     
 Idle Time Out  (1-1000 minutes)

Parameter	Description
Obtain an IP address	The ISP requires you to obtain an IP address by DHCP automatically before connecting to the PPTP server.
Use the following IP Address	The ISP give you a static IP to be used to connect IP address to the PPTP server
IP Address	This is the IP address that your ISP has given you to establish a PPTP connection
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0)
Gateway	Enter the IP address of the ISP Gateway
User ID	Enter the User Name provided by your ISP for the PPTP connection. Sometimes called a Connection ID
Password	Enter the Password provided by your ISP for the PPTP connection
PPTP Gateway	If your LAN has a PPTP gateway, then enter that PPTP gateway IP address here. If you do not have a PPTP gateway then enter the ISP's Gateway IP address above
Connection ID	This is the ID given by ISP. This is optional.



BEZEQ-ISRAE	Select this item if you are using the service provided by BEZEQ in Israel.
Connection Type	<p>If you select "Continuous", the router will always connect to the ISP. If the WAN line breaks down and links again, the router will auto-reconnect to the ISP.</p> <p>If you select "Connect On Demand", the router will auto-connect to the ISP when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "Idle Time".</p> <p>If you select "Manual", the router will connect to ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not be disconnected due to the idle timeout. If the WAN line breaks down and later links again, the router will not auto-connect to the ISP.</p>
Idle Time	<p>You can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent (no one using the Internet) throughout this specified period, then the router will automatically disconnect the connection with your ISP.</p> <p><b>Note:</b> This "idle timeout" function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly when you use this function in the first time, especially your ISP charges you by time used.</p>

Click **<OK>** when you have finished the configuration above. **Congratulations!** You have completed the configuration for the PPTP connection. You can start using the router now, if you wish to use some of the advanced features supported by this router see chapter 2, 3, 4.

### 1.5 L2TP

Select L2TP if your ISP requires the L2TP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.

**L2TP**  
Layer Two Tunneling Protocol is a common connection method used in xDSL connections.

• **WAN Interface Settings**

☒ **Obtain an IP address automatically**

Host Name

MAC address

☐ **Use the following IP address**

IP address

Subnet Mask

Default Gateway

• **L2TP Settings**

User ID

Password

L2TP Gateway

MTU  (512<=MTU Value<=1492)

Connection Type

Idle Time Out  (1-1000 minutes)

Parameter	Description
Obtain an IP address	The ISP requires you to obtain an IP address by DHCP automatically before connecting to the L2TP server.
MAC Address	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this MAC address in this section or use the "Clone MAC Address" button to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work). To find out the PC's MAC address see Appendix A. (see Glossary for an explanation on MAC address)
Use the following IP Address	The ISP gives you a static IP to be used to connect to the L2TP server.
IP Address	This is the IP address that your ISP has given you to establish a L2TP connection.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0)
Gateway	Enter the IP address of the ISP Gateway
User ID	Enter the User Name provided by your ISP for the PPTP connection. Sometimes called a Connection ID
Password	Enter the Password provided by your ISP for the PPTP connection
L2TP Gateway	If your LAN has a L2TP gateway, then enter that L2TP gateway IP address here. If you do not have a L2TP gateway then enter the ISP's Gateway IP address above
MTU	This is optional. You can specify the maximum size of your transmission packet to the Internet. Leave it as it is if you do not wish to set a maximum packet size.

Connection Type	<p>If you select "Continuous", the router will always connect to the ISP. If the WAN line breaks down and links again, the router will auto-reconnect to the ISP.</p> <p>If you select "Connect On Demand", the router will auto-connect to the ISP when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "Idle Time".</p> <p>If you select "Manual", the router will connect to ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not be disconnected due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP.</p>
Idle Time Out	<p>The WAN "idle timeout" auto-disconnect function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. This function also may not work with some ISP. So please make sure this function can work properly when you use this function in the first time, especially your ISP charge you by time used. Due to the many uncontrollable issues, we do not guarantee the WAN "idle timeout" auto-disconnect function will always work. In order to prevent from extra fee charged by ISP, please <b>TURN OFF THE ROUTER WHEN YOU FINISHED USING THE INTERNET.</b></p>

Click <OK> when you have finished the configuration above. **Congratulations!** You have completed the configuration for the L2TP connection. You can start using the router now, if you wish to use some of the advance features supported by this router see chapter 2, 3, 4.

## 1.6 Telstra Big Pond

Select Telstra Big Pond if your ISP requires the Telstra Big Pond protocol to connect you to the Internet. Your ISP should provide all the information required in this section. Telstra Big Pond protocol is used by the ISP in Australia.

Parameter	Description
User Name	Enter the User Name provided by your ISP for the Telstra Big Pond connection
Password	Enter the Password provided by your ISP for the Telstra Big Pond connection
User decide login server manually	Select if you want to assign the IP of Telstra Big Pond's login server manually.
Login Server	The IP of the Login Server.

Click <OK> when you have finished the configuration above. **Congratulations!** You have completed the configuration for the Telstra Big Pond connection. You can start using the router now, if you wish to use some of the advance features supported by this router see chapter 2, 3, 4.

## Chapter 2

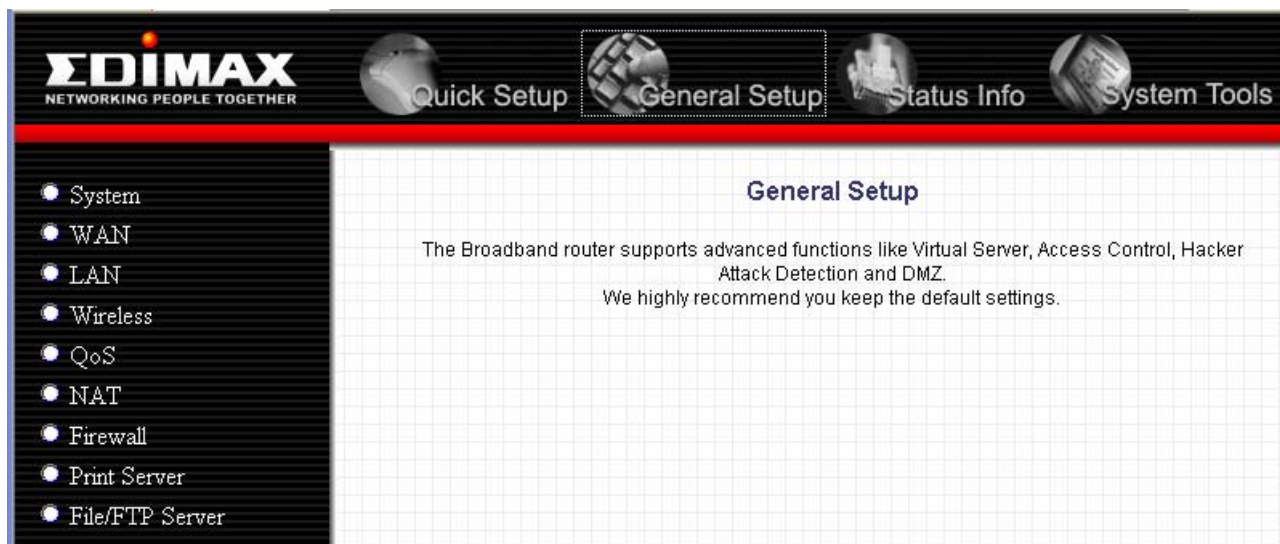
### General Settings

Once you click on the **General Setup** button at the Home Page, you should see the screen below.

If you have already configured the Quick Setup Wizard you do NOT need to configure anything thing in the General Setup screen for you to start using the Internet.

The General Setup contains advanced features that allow you to configure the router to meet your network's needs such as: Wireless, Address Mapping, Virtual Server, Access Control, Hacker Attack Prevention, Special Applications, DMZ and other functions.

Below is a general description of what advance functions are available for this broadband router



Menu	Description
System	This section allows you to set the Broadband router's system Time Zone, Password and Remote Management Administrator.
WAN	This section allows you to select the connection method in order to establish a connection with your ISP (same as the Quick Setup Wizard section)
LAN	You can specify the LAN segment's IP address, subnet Mask, enable/disable DHCP and select an IP range for your LAN
Wireless	Setup the wireless LAN's SSID, WEP key, MAC filtering.
QoS	You can setup the QoS bandwidth control policy.
NAT	You can configure the Address Mapping, Virtual Server and Special Applications functions in this section. This allows you to specify what user/packet can pass your router's NAT.
Firewall	The Firewall section allows you to configure Access Control, Hacker Prevention and DMZ.
Print Server	The Print section allows you to enable the USB ports to support USB printer.
File/FTP Server	The NAS section allows you to enable the USB ports to support USB storage devices.

Select one of the above General Setup selections and proceed to the manual's relevant sub-section

## 2.1 System

The system screen allows you to specify a time zone, to change the system password and to specify a remote management user for the broadband router.

Parameters	Description
Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection
Password Settings	Allows you to select a password in order to access the web-based management website.
Remote Management	You can specify a Host IP address that can perform remote management functions.

Select one of the above three system settings selections and proceed to the manual's relevant sub-section

### 2.1.1 Time Zone

The Time Zone allows your router to reference or base its time on the settings configured here, which will affect functions such as Log entries and Firewall settings.

Parameter	Description
Set Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.



Time Server Address	The router default the "Time Server Address" is "192.43.244.18"
Daylight Savings	The router can also take Daylight savings into account. If you wish to use this function, you must check/tick the enable box to enable your daylight saving configuration (below).
Times From	Select the period in which you wish to start daylight Savings Time
Times to	Select the period in which you wish to end daylight Savings Time

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

### 2.1.2 Password Settings

You can change the password required to log into the broadband router's system web-based management. By default, there is no password. So please assign a password to the Administrator as soon as possible, and store it in a safe place. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.

**EDIMAX**  
NETWORKING PEOPLE TOGETHER

Quick Setup General Setup Status Info System Tools

**System**  
 • Time Zone  
 • Password Settings  
 • Remote Management  
 • WAN  
 • LAN  
 • Wireless  
 • QoS  
 • NAT  
 • Firewall  
 • Print Server  
 • File/FTP Server

### Password Settings

You can change the password required to log into the broadband router's system web-based management. By default, the password is 1234. So please assign a password to the Administrator as soon as possible, and store it in a safe place. Passwords can contain 0 to 30 alphanumeric characters, and are case sensitive.

Current Password	<input type="text"/>
New Password	<input type="text"/>
Confirmed Password	<input type="text"/>

Apply Cancel

Parameters	Description
Current Password	Enter your current password for the remote management administrator to login to your Broadband router. <b>Note:</b> By default there is NO password
New Password	Enter your new password
Confirmed Password	Enter your new password again for verification purposes <b>Note:</b> If you forget your password, you'll have to reset the router to the factory default (No password) with the reset button (see router's back panel)

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

### 2.1.3 Remote Management

The remote management function allows you to designate a host in the Internet the ability to configure the Broadband router from a remote site. Enter the designated host IP Address in the Host IP Address field.



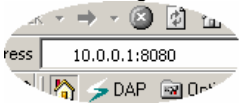
Quick Setup
General Setup
Status Info
System Tools

- System
- Time Zone
- Password Settings
- Remote Management
- WAN
- LAN
- Wireless
- QoS
- NAT
- Firewall
- Print Server
- File/FTP Server

### Remote Management

The remote management function allows you to designate a host in the Internet to have management/configuration access to the Broadband router from a remote site. Enter the designated host IP Address in the Host IP Address field.

Host Address	Port	Enabled
0.0.0.0	8080	<input type="checkbox"/>

Parameters	Description
Host Address	<p>This is the IP address of the host in the Internet that will have management/configuration access to the Broadband router from a remote site. This means if you are at home and your home IP address has been designated the Remote Management host IP address for this router (located in your company office), then you are able to configure this router from your home. If the Host Address is left <b>0.0.0.0</b> this means anyone can access the router's web-based configuration from a remote location, providing they know the password.</p> <p>Click the <b>Enabled</b> box to enable the Remote Management function.</p> <p><b>Note:</b> When you want to access the web-based management from a remote site, you must enter the router's WAN IP address (e.g. 10.0.0.1) into your web-browser followed by port number 8080, e.g. 10.0.0.1:8080 (see below). You'll also need to know the password set in the Password Setting screen in order to access the router's web-based management.</p> 
Port	The port number of remote management web interface.
Enabled	Select "Enabled" to enable the remote management function.

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

## 2.2 WAN

Use the WAN Settings screen if you have already configured the Quick Setup Wizard section and you would like to change your Internet connection type. The WAN Settings screen allows to specify the type of WAN port connect you want to establish with your ISP. The WAN settings offer the following selections for the router's WAN port, **Dynamic IP**, **Static IP Address**, **PPPoE**, **PPTP**, **L2TP**, **Telstra Big Pond**, **DNS** and **DDNS**.

- System
- WAN**
  - Dynamic IP
  - Static IP
  - PPPoE
  - PPTP
  - L2TP
  - Telstra Big Pond
  - DNS
  - DDNS
- LAN
- Wireless
- QoS
- NAT
- Firewall
- Print Server
- File/FTP Server

### WAN Settings

The Broadband router can be connected to your Service Provider through the following methods

<input checked="" type="radio"/> <b>Dynamic IP</b>	Obtains an IP Address automatically from your Service Provider.
<input type="radio"/> <b>Static IP</b>	Uses a Static IP Address. Your Service Provider gives a Static IP Address to access Internet services.
<input type="radio"/> <b>PPPoE</b>	PPP over Ethernet is a common connection method used in xDSL connections.
<input type="radio"/> <b>PPTP</b>	Point-to-Point Tunneling Protocol is a common connection method used in xDSL connections.
<input type="radio"/> <b>L2TP</b>	Layer Two Tunneling Protocol is a common connection method used in xDSL connections.
<input type="radio"/> <b>Telstra Big Pond</b>	Telstra Big Pond is an internet service provided in Australia.

[More Configuration](#)

Parameters	Description
Dynamic IP	Your ISP will automatically give you an IP address
Static IP	Your ISP has given you an IP address already
PPPoE	Your ISP requires PPPoE connection.
PPTP	Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection.
L2TP	Your ISP requires L2TP connection.
Telstra Big Pond	Your ISP requires Telstra Big Pond connection.
DNS	You can specify a DNS server that you wish to use
DDNS	You can specify a DDNS server that you wish to use and configure the user name and password provided by you DDNS service provider.

Once you have made a selection, click **<More Configuration>** at the bottom of the screen and proceed to the manual's relevant sub-section



### 2.2.1 Dynamic IP

Choose the Dynamic IP selection if your ISP will automatically give you an IP address. Some ISP's may also require that you fill in additional information such as Host Name, Domain Name and MAC address (see chapter 1 "Cable Modem" for more detail)

### 2.2.2 Static IP Address

Select Static IP address if your ISP has given you a specific IP address for you to use. Your ISP should provide all the information required in this section. (See chapter 1 "Fixed IP" for more detail)

### 2.2.3 PPPoE (PPP over Ethernet)

Select PPPoE if your ISP requires the PPPoE protocol to connect you to the Internet. Your ISP should provide all the information required in this section. (See chapter 1 "PPPoE" for more detail)

### 2.2.4 PPTP

Select PPTP if your ISP requires the PPTP protocol to connect you to the Internet. Your ISP should provide all the information required in this section. (See chapter 1 "PPTP" for more detail)

### 2.2.5 L2TP

Select L2TP if your ISP requires the L2TP protocol to connect you to the Internet. Your ISP should provide all the information required in this section. (See chapter 1 "L2TP" for more detail)

### 2.2.6 Telstra Big Pond

Select Telstra Big Pond if your ISP requires the Telstra Big Pond protocol to connect you to the Internet. Your ISP should provide all the information required in this section. Telstra Big Pond protocol is used by the ISP in Australia. (See chapter 1 "Telstra Big Pond" for more detail)

### 2.2.7 DNS

A Domain Name System (DNS) server is like an index of IP addresses and Web addresses. If you type a Web address into your browser, such as [www.router.com](http://www.router.com), a DNS server will find that name in its index and the matching IP address. Most ISPs provide a DNS server for speed and convenience. If your Service Provider connects you to the Internet with dynamic IP settings, it is likely that the DNS server IP address is provided automatically. However, if there is a DNS server that you would rather use, you need to specify the IP address of that DNS server here.

**EDIMAX**  
NETWORKING PEOPLE TOGETHER

Quick Setup General Setup Status Info System Tools

System  
WAN  
Dynamic IP  
Static IP  
PPPoE  
PPTP  
L2TP  
Telstra Big Pond  
DNS  
DDNS  
LAN  
Wireless  
QoS  
NAT  
Firewall  
Print Server  
File/FTP Server

### DNS

A Domain Name System (DNS) server is like an index of IP Addresses and Web Addresses. If you type a Web address into your browser, such as [www.broadbandrouter.com](http://www.broadbandrouter.com), a DNS server will find that name in its index and find the matching IP address. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect you to the Internet through dynamic IP settings, it is likely that the DNS server IP Address is also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP Address of that DNS server. The primary DNS will be used for domain name access first, in case the primary DNS access failures, the secondary DNS will be used.  
Has your Internet service provider given you a DNS address?

DNS address

Secondary DNS Address (optional)

Apply Cancel

Parameters	Description
DNS address	This is the ISP's DNS server IP address that they gave you; or you can specify your own preferred DNS server IP address
Secondary DNS Address (optional)	This is optional. You can enter another DNS server's IP address as a backup. The secondary DNS will be used should the above DNS fail.

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

### 2.2.8 DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. This router supports DynDNS, TZO and other common DDNS service providers.

**EDIMAX**  
NETWORKING PEOPLE TOGETHER

Quick Setup General Setup Status Info System Tools

System  
WAN  
Dynamic IP  
Static IP  
PPPoE  
PPTP  
L2TP  
Telstra Big Pond  
DNS  
DDNS  
LAN  
Wireless  
QoS  
NAT  
Firewall  
Print Server  
File/FTP Server

### DDNS

DDNS allows users to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. Our products have DDNS support for [www.dyndns.org](http://www.dyndns.org) and [www.tzo.com](http://www.tzo.com) now.

Dynamic DNS	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Provider	DynDNS
Domain Name	
Account / E-Mail	
Password / Key	






Apply Cancel

Parameters	Default	Description
Enable/Disable	Disable	Enable/Disable the DDNS function of this router
Provider	—	Select a DDNS service provider
Domain name	—	Your static domain name that use DDNS
Account/E-mail	—	The account that your DDNS service provider assigned to you
Password/Key	—	The password you set for the DDNS service account above

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

### 2.3 LAN

The LAN Port screen below allows you to specify a private IP address for your router's LAN ports as well as a subnet mask for your LAN segment.

- System
- WAN
- LAN**
- Wireless
- QoS
- NAT
- Firewall
- Print Server
- File/FTP Server

### LAN Settings

The router default IP address is 192.168.2.1. You can change it according to your network. DHCP server is to assign IP address to PCs connected to the router. You can disable this feature.

#### LAN IP

IP address	192.168.2.1
Subnet Mask	255.255.255.0
802.1d Spanning Tree	Disabled
DHCP Server	Enabled

#### DHCP Server

Lease Time	Forever
Start IP	192.168.2.100
End IP	192.168.2.200
Domain Name	

Parameters	Default	Description
LAN IP	—	
IP address	192.168.2.1	This is the router's LAN port IP address (Your LAN clients default gateway IP address)
IP Subnet Mask	255.255.255.0	Specify a Subnet Mask for your LAN segment
802.1d Spanning Tree	Disabled	If 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent from network loop happened in the LAN ports.
DHCP Server	Enabled	You can enable or disable the DHCP server. By enabling the DHCP server the router will automatically give your LAN clients an IP address. If the DHCP is not enabled then you'll have to manually set your LAN client's IP addresses; make sure the LAN Client is in the same subnet as this broadband router if you want the router to be your LAN client's default gateway
Lease Time	Forver	The DHCP when enabled will temporarily give your LAN clients an IP address. In the Lease Time setting you can specify the time period that the DHCP lends an IP address to your LAN clients. The DHCP will change your LAN client's IP address when this time threshold period is reached
IP Address Pool	—	You can select a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients. <b>Note:</b> By default the IP range is from: Start IP <b>192.168.2.100</b> to End IP <b>192.168.2.200</b> . If you want your PC to have a static/fixed IP address then you'll have to choose an IP address outside this IP address Pool.
Domain Name	—	You can specify a Domain Name for your LAN.

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

## 2.4 Wireless

Wireless Access Point builds a wireless LAN and can let all PCs equipped with IEEE 802.11b or 801.11g wireless network adaptor connect to your Intranet. It supports WEP and WPA2 encryption to enhance the security of your wireless network.

**EDIMAX**  
NETWORKING PEOPLE TOGETHER

Quick Setup General Setup Status Info System Tools

System  
WAN  
LAN  
Wireless  
Basic Settings  
Advance Settings  
Security Settings  
Access Control  
QoS  
NAT  
Firewall  
Print Server  
File/FTP Server

### Wireless Settings

In order to utilize the Router's wireless functions, select Enable. If you prefer not to utilize any wireless functions, make sure Disable is selected. (Note: No other wireless functions will be available unless you enable this setting.)

Enable or disable Wireless module function : ☒ Enable ☐ Disable

Apply

Parameters	Default	Description
Enable or disable Wireless module function	Enable	You can select to enable or disable the wireless access point module of this router.

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

### 2.4.1 Basic Settings

You can set parameters that are used for the wireless stations to connect to this router. The parameters include Mode, ESSID, Channel Number and Associated Client.

#### Setting Page

**EDIMAX**  
NETWORKING PEOPLE TOGETHER

Quick Setup General Setup Status Info System Tools

System  
WAN  
LAN  
Wireless  
Basic Settings  
Advance Settings  
Security Settings  
Access Control  
QoS  
NAT  
Firewall  
Print Server  
File/FTP Server

### Wireless Settings

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode :	AP
Band :	2.4 GHz (B+G)
ESSID :	default
Channel Number :	11

Apply Cancel

Parameters	Default	Description
Mode	AP	It allows you to set the AP to AP, Bridge or WDS mode.
Band	2.4GHz(B+G)	It allows you to set the AP fix at 802.11b or 802.11g mode. You also can select B+G mode to allow the AP select 802.11b and 802.11g connection automatically.
ESSID	default	This is the name of the wireless LAN. All the devices in the same wireless LAN should have the same ESSID.
Channel Number	11	The channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel.
MAC address	—	If you want to bridge more than one network together with wireless LAN, you have to set this access point to “AP Bridge-Point to Point mode”, “AP Bridge-Point to Multi-Point mode” or “AP Bridge-WDS mode”. You have to enter the MAC addresses of other access points that join the bridging work.
Set Security	—	Click the “Set Security” button, and then a “WDS Security Settings” will pop up. You can set the security parameters used to bridge access points together here when your AP is in AP Bridge modes. You can refer to section 4.3 “Security Settings” for how to set the parameters.

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)



### 2.4.2 Advanced Settings

You can set advanced wireless LAN parameters of this router. The parameters include Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval, preamble Type ..... You should not change these parameters unless you know what effect the changes will have on this router.

**EDIMAX**  
NETWORKING PEOPLE TOGETHER

Quick Setup General Setup Status Info System Tools

**Advanced Settings**

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router.

Fragment Threshold:	2346	(256-2346)
RTS Threshold:	2347	(0-2347)
Beacon Interval:	100	(20- 1024 ms)
DTIM Period:	3	(1-10)
Data Rate:	Auto	
Preamble Type:	<input checked="" type="radio"/> Long Preamble	<input type="radio"/> Short Preamble
Broadcast Essid :	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
CTS Protect:	<input type="radio"/> Auto	<input type="radio"/> Always <input checked="" type="radio"/> None
Tx Power:	100 %	
Turbo Mode:	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
WMM :	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable

Apply Cancel

Parameters	Description
Fragment Threshold	"Fragment Threshold" specifies the maximum size of packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.
RTS Threshold	When the packet size is smaller the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.
Beacon Interval	The interval of time that this wireless router broadcast a beacon. Beacon is used to synchronize the wireless network.
DTIM Period	The DTIM period you specify here indicates how often the clients served by this access point should check for buffered data still on the AP awaiting pickup.
Data Rate	The "Data Rate" is the rate this access point uses to transmit data packets. The access point will use the highest possible selected transmission rate to transmit the data packets.
Preamble Type	The "Long Preamble" can provide better wireless LAN compatibility while the "Short Preamble" can provide better wireless LAN performance.
Broadcast ESSID	If you enable "Broadcast ESSID", every wireless station located within the coverage of this access point can discover this access point easily. If you are building a public wireless network, enabling this feature is recommended. Disabling "Broadcast ESSID" can provide better security.
IAPP	If you enable "IAPP", it will allow wireless station roaming between IAPP enabled access points within the same wireless LAN.
CTS Protect	It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to many of frame traffic should be transmitted.
Tx Power	You can adjust the wireless transmit power here. By reduce the tx power can let the wireless signal only cover your working area.

Turbo Mode	By enable the turbo mode can enhance the throughput up to 35Mbps.
WMM	WMM stands for Wi-Fi Multimedia. It is a standard created to define quality of service (QoS) in Wi-Fi networks. This adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources.

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router.

### 2.4.3 Security

This Router provides complete wireless LAN security functions, include WEP, IEEE 802.11x, IEEE 802.11x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function.

#### 2.4.3.1 WEP only

When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You can enter four WEP keys and select one of them as default key. Then the router can receive any packets encrypted by one of the four keys

Parameters	Default	Description
Key Length	64-bit	You can select the WEP key length for encryption, 64-bit or 128-bit. Larger WEP key length will provide higher level of security, but the throughput will be lower.
Key Format	—	You may to select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key. For example: ASCII Characters: guest Hexadecimal Digits: 12345abcde
Default Key	Key 1	Select one of the four keys to encrypt your data. Only the key you select it in the "Default key" will take effect.
Key 1 - Key 4	—	The WEP keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules: 64-bit WEP: input 10-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII



		character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 13-digit ASCII characters as the encryption keys.
--	--	---

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

#### 2.4.3.2 802.1x only

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encryption the data during communication.

**EDIMAX**  
NETWORKING PEOPLE TOGETHER

Quick Setup General Setup Status Info System Tools

System  
WAN  
LAN  
Wireless  
    Basic Settings  
    Advance Settings  
    Security Settings  
    Access Control  
QoS  
NAT  
Firewall  
Print Server  
File/FTP Server

### Security Settings

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption : Disable

☒ **Enable 802.1x Authentication**

RADIUS Server IP address :

RADIUS Server Port : 1812

RADIUS Server Password :






Apply Cancel

Parameters	Description
RADIUS Server IP address	The IP address of external RADIUS server.
RADIUS Server Port	The service port of the external RADIUS server.
RADIUS Server Password	The password used by external RADIUS server.

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

#### 2.4.3.3 802.1x WEP Static key

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode also uses WEP to encrypt the data during communication.

- System
- WAN
- LAN
- Wireless
  - Basic Settings
  - Advance Settings
  - Security Settings
  - Access Control
- QoS
- NAT
- Firewall
- Print Server
- File/FTP Server

### Security Settings

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption :	WEP
Key Length :	64-bit
Key Format :	Hex (10 characters)
Default Key :	Key 1
Encryption Key 1 :	*****
Encryption Key 2 :	*****
Encryption Key 3 :	*****
Encryption Key 4 :	*****
<input checked="" type="checkbox"/> Enable 802.1x Authentication	
RADIUS Server IP address :	
RADIUS Server Port :	1812
RADIUS Server Password :	

For the WEP settings please refer to section 2.4.3.1 “WEP only”. For the 802.1x settings, please refer to section 2.4.3.2 “802.1x only”.

#### 2.4.3.4 WPA Pre-shared key

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be broken by hackers. This can improve security very much.


The screenshot shows the EDIMAX router's web interface. The top navigation bar includes 'Quick Setup', 'General Setup', 'Status Info', and 'System Tools'. The left sidebar lists various settings: System, WAN, LAN, Wireless (selected), Basic Settings, Advance Settings, Security Settings (highlighted), and Access Control. Below these are QoS, NAT, Firewall, Print Server, and File/FTP Server. The main content area is titled 'Security Settings' and contains a descriptive paragraph about wireless security. Below the text are four configuration rows: 'Encryption' set to 'WPA pre-shared key', 'WPA Unicast Cipher Suite' with radio buttons for 'WPA(TKIP)' (selected), 'WPA2(AES)', and 'WPA2 Mixed'; 'Pre-shared Key Format' set to 'Passphrase'; and 'Pre-shared Key' with an empty text box. 'Apply' and 'Cancel' buttons are at the bottom right.

Parameters	Description
WPA(TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
WPA2(AES)	This use CCMP protocol to change encryption key frequently. AES can provide high level encryption to enhance the wireless LAN security.
WPA2 Mixed	This will use TKIP or AES based on the other communication peer automatically.
Pre-shared Key Format	You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the Pre-shared Key. For example: Passphrase: iamguest Hexadecimal Digits: 12345abcde
Pre-shared Key	The Pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill the text box by following the rules below. Hex WEP: input 64-digit Hex values (in the "A-F", "a-f" and "0-9" range) or at least 8 character pass phrase as the pre-shared keys.

Click <Apply> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

#### 2.4.3.5 WPA Radius

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. This can improve security very much.



Quick Setup
General Setup
Status Info
System Tools

- ☐ System
- ☐ WAN
- ☐ LAN
- ☒ Wireless
  - ☒ Basic Settings
  - ☐ Advance Settings
  - ☐ Security Settings
  - ☐ Access Control
- ☐ QoS
- ☐ NAT
- ☐ Firewall
- ☐ Print Server
- ☐ File/FTP Server

### Security Settings

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption :	WPA RADIUS
WPA Unicast Cipher Suite :	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
RADIUS Server IP address :	<input type="text"/>
RADIUS Server Port :	1812
RADIUS Server Password :	<input type="text"/>

Parameters	Description
WPA(TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
WPA2(AES)	This use CCMP protocol to change encryption key frequently. AES can provide high level encryption to enhance the wireless LAN security.
WPA2 Mixed	This will use TKIP or AES based on the other communication peer automatically.
RADIUS Server IP address	The IP address of external RADIUS server.
RADIUS Server Port	The service port of the external RADIUS server.
RADIUS Server Password	The password used by external RADIUS server.

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

#### 2.4.4 Access Control

This wireless router provides MAC Address Control, which prevents the unauthorized MAC Addresses from accessing your wireless network.

Quick Setup
General Setup
Status Info
System Tools

- System
- WAN
- LAN
- **Wireless**
  - Basic Settings
  - Advance Settings
  - Security Settings
  - **Access Control**
- QoS
- NAT
- Firewall
- Print Server
- File/FTP Server

### MAC Address Filtering

For security reason, the Access Point features MAC Address Filtering that only allows authorized MAC Addresses associating to the Access Point.

● **MAC Address Filtering Table**  
It allows to entry 20 sets address only.

NO.	MAC address	Comment	Select
<div style="display: flex; justify-content: space-around; margin-top: 5px;"> <span>Delete Selected</span> <span>Delete All</span> <span>Reset</span> </div>			

☐ **Enable Wireless Access Control**

New

MAC address :

Comment:

Add

Reset

Apply
Cancel

Parameters	Description
Enable wireless access control	Enable wireless access control
Add MAC address into the list	Fill in the "MAC Address" and "Comment" of the wireless station to be added and then click "Add". Then this wireless station will be added into the "Current Access Control List" below. If you find any issues before adding it and want to retype again. Just click "Clear" and both "MAC Address" and "Comment" fields will be cleared.
Remove MAC address from list	If you want to remove some MAC address from the "Current Access Control List ", select the MAC addresses you want to remove in the list and then click "Delete Selected". If you want remove all MAC addresses from the table, just click "Delete All" button. Click "Reset" will clear your current selections.






Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

## 2.5 QoS

The QoS can let you classify Internet application traffic by source/destination IP address and port number. You can assign priority for each type of application and reserve bandwidth for it. The packets of applications with higher priority will always go first. Lower priority applications will get bandwidth after higher priority applications get enough bandwidth. This can let you have a better experience in using critical real time services like Internet phone, video conference ...etc. All the applications not specified by you are classified as rule name "Others". The rule with smaller priority number has higher priority; the rule with larger priority number has lower priority. You can adjust the priority of the rules by moving them up or down.

Note: If the total assigned bandwidth of higher priority applications is larger than the maximum bandwidth provided by the WAN port, the other applications will not get any bandwidth.



- System
- WAN
- LAN
- Wireless
- QoS**
- NAT
- Firewall
- Print Server
- File/FTP Server

### QoS

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail.

☐ **Enable QoS**

Total Download Bandwidth :  **kbits**

Total Upload Bandwidth :  **kbits**

Current QoS Table				
Priority	Rule Name	Upload Bandwidth	Download Bandwidth	Select
<div> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Move Up"/> </div> <div> <input type="button" value="Move Down"/> <input type="button" value="Reset"/> </div>				

Parameters	Description
Enable/Disable QoS	You can check "Enable QoS" to enable QoS function for the WAN port. You also can uncheck "Enable QoS" to disable QoS function for the WAN port.
Total Download Bandwidth	Here you can set maximum download bandwidth for all the users of the router sharing.
Total Upload Bandwidth	Here you can set the maximum upload bandwidth for all the users of the router sharing.
Add a QoS rule into the table	Click "Add" then you will enter a form of the QoS rule. Click "Apply" after filling out the form and the rule will be added into the table.
Remove QoS rules from table	If you want to remove some QoS rules from the table, select the QoS rules you want to remove in the table and then click "Delete Selected". If you want remove all QoS rules from the table, just click "Delete All" button. Click "Reset" will clear your current selections.
Edit a QoS rule	Select the rule you want to edit and click "Edit", then you will enter the detail form of the QoS rule. Click "Apply" after editing the form and the rule will be saved.
Adjust QoS rule priority	You can select the rule and click "Move Up" to make its priority higher. You also can select the rule and click "Move Down" to make its priority lower.

#### Edit QoS Rule:

You can assign packet classification criteria by its local IP range, remote IP range, traffic type, protocol, local port range and remote port range parameters. The parameters that you leave as blank will be ignored. The priority of this rule will be applied to packets that match classification criteria of this rule. You can limit bandwidth consumed by packets that match this rule or guarantee bandwidth required by packets that match this rule.

**EDIMAX**  
NETWORKING PEOPLE TOGETHER

Quick Setup

General Setup

Status Info

System Tools

- ☐ System
- ☐ WAN
- ☐ LAN
- ☐ Wireless
- ☒ QoS
- ☐ NAT
- ☐ Firewall
- ☐ Print Server
- ☐ File/FTP Server

### QoS

This page allows users to add/modify the QoS rule's settings.

Rule Name :	<input style="width: 100%;" type="text"/>
Bandwidth :	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 5px;">Download</div> <div style="border: 1px solid #ccc; width: 80px; height: 20px; margin: 0 5px;"></div> <div style="margin: 0 5px;">Kbps</div> <div style="border: 1px solid #ccc; padding: 2px 5px;">guarantee</div> </div>
Local IP address :	<input style="width: 40%;" type="text"/> - <input style="width: 40%;" type="text"/>
Local Port Range :	<input style="width: 100%;" type="text"/>
Remote IP address :	<input style="width: 40%;" type="text"/> - <input style="width: 40%;" type="text"/>
Remote Port Range :	<input style="width: 100%;" type="text"/>
Traffic Type :	<div style="border: 1px solid #ccc; padding: 2px 5px;">None</div>
Protocol :	<div style="border: 1px solid #ccc; padding: 2px 5px;">TCP</div>

Save...

Reset

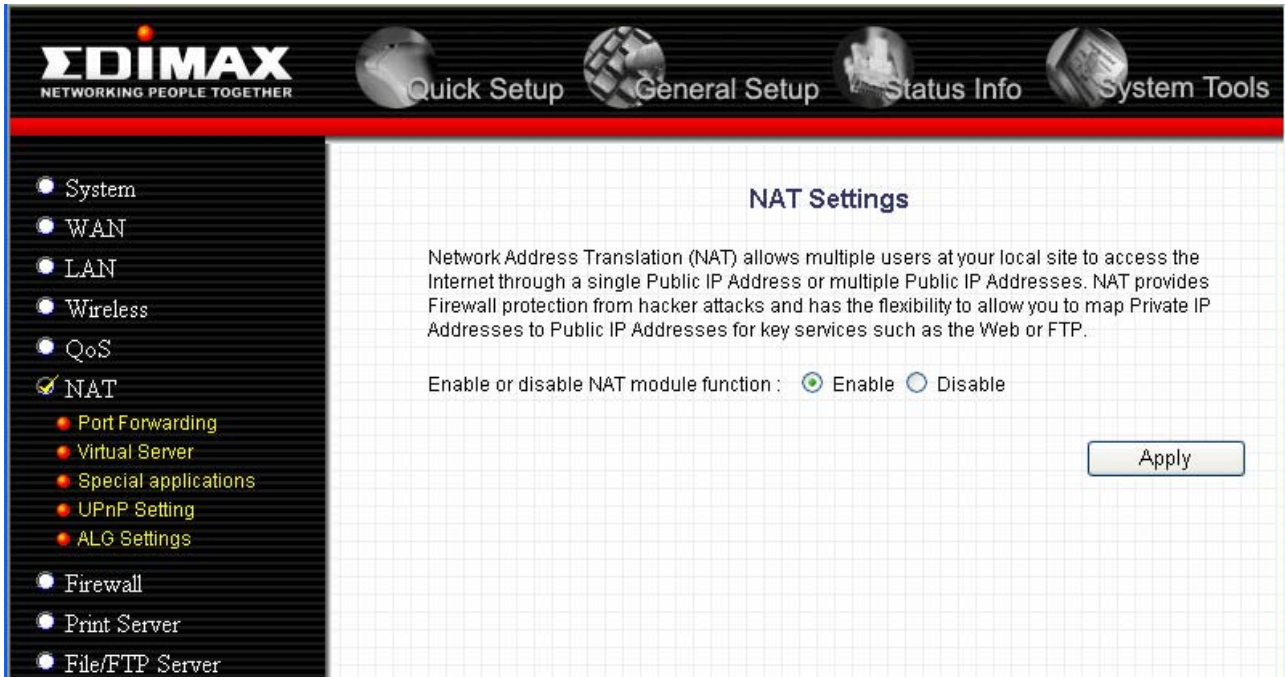
Parameters	Description
Rule Name	The name of this rule.
Bandwidth	You can assign the download or upload bandwidth by the unit of Kbps (1024 bit per second). You can limit the maximum bandwidth consumed by this rule by selecting "Maximum". You also can reserve enough bandwidth for this rule by selecting "Guarantee".
Local IP Address	Enter the local IP address range of the packets that this rule will apply to. If you assign 192.168.2.3 – 192.168.2.5, it means 3 IP addresses: 192.168.2.3, 192.168.2.4 and 192.168.2.5
Local Port Range	Enter the local port range of the packets that this rule will apply to. You can assign a single port number here or assign a range of port numbers by assigning the first port number and the last port number of the range. The two numbers are separated by a dash "-", for example "101-150" means from port number 100 to port number 150 – the range of 50 port numbers.
Remote IP Address	Enter the remote IP address range of the packets that this rule will apply to. If you assign 192.168.2.3 – 192.168.2.5, it means 3 IP addresses: 192.168.2.3, 192.168.2.4 and 192.168.2.5
Remote Port Range	Enter the remote port range of the packets that this rule will apply to. You can assign a single port number here or assign a range of port numbers by assigning the first port number and the last port number of the range. The two numbers are separated by a dash "-", for example "101-150" means from port number 100 to port number 150 – the range of 50 port numbers.
Traffic Type	Select the traffic type of the packets that this rule will apply to. We list some popular applications here to ease the configuration. You also can get the same result by using other parameters, for example source or destination port number, if you are familiar with the application protocol.
Protocol	Select the protocol type of the packets that this rule will apply to.
Apply	Apply and exit the form.
Reset	Clear the content of this form.

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)



## 2.6 NAT

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP.




Parameters	Description
Port Forwarding	You can have different services (e.g. email, FTP, Web etc.) going to different service servers/clients in your LAN. The Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address.
Virtual Server	You can have different services (e.g. email, FTP, Web etc.) going to different service servers/clients in your LAN. The Virtual Server allows you to re-direct a particular service port number (from the Internet/WAN Port) to a particular LAN IP address and its service port number.
Special Applications	Some applications require multiple connections, such as Internet games, video conferencing, Internet telephony and others. In this section you can configure the router to support these types of applications.
UPnP Setting	It allows to Enable or Disable UPnP feature here. After you enable the UPnP feature, all client systems that support UPnP, like Windows XP, can discover this router automatically and access the Internet through this router without any configuration. The NAT Traversal function provided by UPnP can let applications that support UPnP smoothly connect to Internet sites without any incompatibility problem due to the NAT port translation.
ALG Setting	You can select special applications that need "Application Layer Gateway" to support here.
Static Routing	You can disable NAT function and setup the routing rules manually.

Click on one of the above NAT selections and proceed to the manual's relevant sub-section.

### 2.6.1 Port Forwarding

The Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address. It helps you to host some servers behind the router NAT firewall.



Quick Setup
General Setup
Status Info
System Tools

- System
- WAN
- LAN
- Wireless
- QoS
- NAT
  - **Port Forwarding**
  - Virtual Server
  - Special applications
  - UPnP Setting
  - ALG Settings
- Firewall
- Print Server
- File/FTP Server

### Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

☐ **Enable Port Forwarding**

Private IP	Type	Port Range	Comment
<input type="text"/>	Both ▼	<input type="text"/> - <input type="text"/>	<input type="text"/>
			<input type="button" value="Add"/> <input type="button" value="Reset"/>

**Current Port Forwarding Table**

NO.	Private IP	Type	Port Range	Comment	Select

Parameters	Description
Enable Port Forwarding	Enable Port Forwarding
Private IP	This is the private IP of the server behind the NAT firewall. <b>Note:</b> You need to give your LAN PC clients a fixed/static IP address for Port Forwarding to work properly.
Type	This is the protocol type to be forwarded. You can choose to forward "TCP" or "UDP" packets only or select "both" to forward both "TCP" and "UDP" packets.
Port Range	The range of ports to be forward to the private IP.
Comment	The description of this setting.
Add Port Forwarding	Fill in the "Private IP", "Type", "Port Range" and "Comment" of the setting to be added and then click "Add". Then this Port Forwarding setting will be added into the "Current Port Forwarding Table" below. If you find any typo before adding it and want to retype again, just click "Clear" and the fields will be cleared.
Remove Port Forwarding	If you want to remove some Port Forwarding settings from the "Current Port Forwarding Table", select the Port Forwarding settings you want to remove in the table and then click "Delete Selected". If you want remove all Port Forwarding settings from the table, just click "Delete All" button. Click "Reset" will clear your current selections.

Click <Apply> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

### 2.6.2 Virtual Server

Use the Virtual Server function when you want different servers/clients in your LAN to handle different service/Internet application type (e.g. Email, FTP, Web server etc.) from the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to re-direct a particular service port number (from the Internet/WAN Port) to a particular LAN private IP address and its service port number. (See Glossary for an explanation on Port number)

Parameters	Description
Enable Virtual Serve	Enable Virtual Server.
Private IP	This is the LAN client/host IP address that the Public Port number packet will be sent to. <b>Note:</b> You need to give your LAN PC clients a fixed/static IP address for Virtual Server to work properly.
Private Port	This is the port number (of the above Private IP host) that the below Public Port number will be changed to when the packet enters your LAN (to the LAN Server/Client IP)
Type	Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default both protocols.
Public Port	Enter the service (service/Internet application) port number from the Internet that will be re-directed to the above Private IP address host in your LAN <b>Note:</b> Virtual Server function will have priority over the DMZ function if there is a conflict between the Virtual Server and the DMZ settings.
Comment	The description of this setting.
Add Virtual Server	Fill in the "Private IP", "Private Port", "Type", "Public Port" and "Comment" of the setting to be added and then click "Add". Then this Virtual Server setting will be added into the "Current Virtual Server Table" below. If you find any typo before adding it and want to retype again, just click "Clear" and the fields will be cleared.
Remove Virtual Server	If you want to remove some Virtual Server settings from the "Current Virtual Server Table", select the Virtual Server settings you want to remove in the table and then click "Delete Selected". If you want remove all Virtual Server settings from the table, just click "Delete All" button. Click "Reset" will clear your current selections.

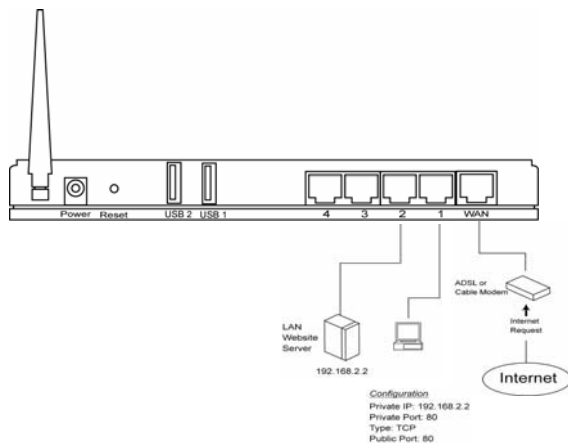
Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

**Note:** The function of NAS FTP/HTTP server will be affected after you setting FTP/HTTP server in Virtual Server, due to the priority of settings in Virtual Server are higher than in NAS.

#### Example: Virtual Server

The diagram below demonstrates one of the ways you can use the Virtual Server function. Use the Virtual Server when you want the web server located in your private LAN to be accessible to Internet users. The configuration below means that any request coming form the Internet to access your web server will be translated to your LAN's web server (192.168.2.2).

**Note:** For the virtual server to work properly Internet/remote users must know your global IP address. (For websites you will need to have a fixed/static global/public IP address)



### 2.6.3 Special Applications

Some applications require multiple connections, such as Internet games, video conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.

The screenshot shows the EDIMAX Special Applications configuration page. The left sidebar contains a navigation menu with options: System, WAN, LAN, Wireless, QoS, NAT (selected), Port Forwarding, Virtual Server, Special applications (highlighted), UPnP Setting, ALG Settings, Firewall, Print Server, and File/FTP Server. The main content area is titled "Special Applications" and includes a description: "Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the 'Trigger Port' field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic. Note: The range of the Trigger Port is 1 to 65535." Below this is a section for "Enable Trigger Port" with a checkbox and a table for configuring trigger ports. The table has columns: Trigger Port, Trigger Type, Public Port, Public Type, and Comment. There are also buttons for "Add" and "Reset". Below the table is a "Current Trigger-Port Table" with columns: NO., Trigger Port, Trigger Type, Public Port, Public Type, Comment, and Select. There are buttons for "Delete Selected", "Delete All", and "Reset". At the bottom right are "Apply" and "Cancel" buttons.

Parameters	Description
Enable Trigger Port	Enable the Special Application function.
Trigger Port	This is the out going (Outbound) range of port numbers for this particular application
Trigger Type	Select whether the outbound port protocol is "TCP", "UDP" or both.
Public Port	Enter the In-coming (Inbound) port or port range for this type of application (e.g. 2300-2400, 47624) <b>Note:</b> Individual port numbers are separated by a comma (e.g. 47624, 5775, and 6541 etc.). To input a port range use a "dash" to separate the two port number range (e.g. 2300-2400)
Public Type	Select the Inbound port protocol type: "TCP", "UDP" or both



Comment	The description of this setting.
Popular applications	This section lists the more popular applications that require multiple connections. Select an application from the Popular Applications selection. Once you have selected an application, select a location (1-10) in the <b>Copy to</b> selection box and then click the <b>Copy to</b> button. This will automatically list the Public Ports required for this popular application in the location (1-10) you'd specified.
Add Special Application	Fill in the "Trigger Port", "Trigger Type", "Public Port", "Public Type", "Public Port" and "Comment" of the setting to be added and then click "Add". Then this Special Application setting will be added into the "Current Trigger-Port Table" below. If you find any typo before adding it and want to retype again, just click "Clear" and the fields will be cleared. If you want to add a popular application, select one "Popular Application" and then click "Add".
Remove Special Application	If you want to remove some Special Application settings from the "Current Trigger-Port Table", select the Special Application settings you want to remove in the table and then click "Delete Selected". If you want remove all Special Applications settings from the table, just click "Delete All" button. Click "Reset" will clear your current selections.

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

#### Example: Special Applications

If you need to run applications that require multiple connections, specify the port (outbound) normally associated with that application in the "Trigger Port" field. Then select the protocol type (TCP or UDP) and enter the public ports associated with the trigger port to open them up for inbound traffic.

#### Example:

ID	Trigger Port	Trigger Type	Public Port	Public Type	Comment
1	28800	UDP	2300-2400, 47624	TCP	MSN Game Zone
2	6112	UDP	6112	UDP	Battle.net

In the example above, when a user trigger's port 28800 (outbound) for MSN Game Zone then the router will allow incoming packets for ports 2300-2400 and 47624 to be directed to that user.

**Note:** Only one LAN client can use a particular special application at a time.

#### 2.6.4 UPnP Settings

With UPnP, all PCs in you Intranet will discover this router automatically. So you do not have to do any configuration for your PC and can access the Internet through this router easily.

**EDIMAX**  
NETWORKING PEOPLE TOGETHER

Quick Setup General Setup Status Info System Tools

System  
WAN  
LAN  
Wireless  
QoS  
NAT  
Port Forwarding  
Virtual Server  
Special applications  
UPnP Setting  
ALG Settings  
Firewall  
Print Server  
File/FTP Server

### UPnP

UPnP is more just a simple extension of the Plug and Play peripheral model. It is designed to support zero-configuration, "invisible" networking, and automatic discovery for a breadth of device categories from a wide range of vendors. With UPnP, a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices-all automatically; truly enabling zero configuration networks. Devices can subsequently communicate with each other directly; thereby further enabling peer to peer networking.

UPnP Feature: ☐ Enable ☒ Disable

Apply Cancel

Parameters	Default	Description
UPnP Feature	Disable	You can Enable or Disable UPnP feature here. After you enable the UPnP feature, all client systems that support UPnP, like Windows XP, can discover this router automatically and access the Internet through this router without any configuration. The NAT Traversal function provided by UPnP can let applications that support UPnP smoothly connect to Internet sites without any incompatibility problem due to the NAT port translation.

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

### 2.6.5 ALG Settings

You can select applications that need "Application Layer Gateway" to support.

Enable	Name	Comment
<input checked="" type="checkbox"/>	Amanda	Support for Amanda backup tool protocol.
<input checked="" type="checkbox"/>	Egg	Support for eggdrop bot networks.
<input checked="" type="checkbox"/>	FTP	Support for FTP.
<input checked="" type="checkbox"/>	H323	Support for H323/netmeeting.
<input checked="" type="checkbox"/>	IRC	Allows DCC to work though NAT and connection tracking.
<input checked="" type="checkbox"/>	MMS	Support for Microsoft Streaming Media Services protocol.
<input checked="" type="checkbox"/>	Quake3	Support for Quake III Arena connection tracking and nat.
<input checked="" type="checkbox"/>	Talk	Allows netfilter to track talk connections.
<input checked="" type="checkbox"/>	TFTP	Support for TFTP.
<input checked="" type="checkbox"/>	Starcraft	Support for Starcraft/Battle.net game protocol.
<input checked="" type="checkbox"/>	MSN	Support for MSN file tranfer.

Parameters	Default	Description
Enable		You can select to enable "Application Layer Gateway", and then the router will let that application correctly pass though the NAT gateway.

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

### 2.6.6 Static Routing

This router provides Static Routing function when NAT is disabled. With Static Routing, the router can forward packets according to your routing rules. The IP sharing function will not work any more in Static Routing mode.

**Note:** The DMZ function of firewall will not work if static routing is enabled.



Parameters	Description
Enable Static Routing	Static Routing function is default disabled. You have to enable the Static Routing function before your routing rules take effect.
Destination LAN IP	The network address of destination LAN.
Subnet Mask	The subnet mask of destination LAN.
Default Gateway	The next stop gateway of the path toward the destination LAN. This is the IP of the neighbor router that this router should communicate with on the path to the destination LAN.
Hop Count	The number of hops (routers) to pass through to reach the destination LAN.
Interface	The interface that go to the next hop (router).
Add a Rule	Fill in the "Destination LAN IP", "Subnet Mask", "Default Gateway", "Hop Count" and "Interface" of the rule to be added and then click "Add". Then this rule of Static Routing will be added into the "Static Routing Table" below. If you find any typo before adding it and want to retype again, just click "Reset" and the fields will be cleared.
Remove a Rule	If you want to remove some routing rules from the "Static Routing Table", select the rules you want to remove in the table and then click "Delete Selected". If you want remove all rules from the table, just click "Delete All" button. Click "Reset" will clear your current selections.

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

## 2.7 Firewall

The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

**Note:** To enable the Firewall settings select **Enable** and click **Apply**







- System
- WAN
- LAN
- Wireless
- QoS
- NAT
- Firewall**
  - Access Control
  - URL Blocking
  - DoS
  - DMZ
- Print Server
- File/FTP Server

### Security Settings (Firewall)

The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).






Enable or disable Firewall module function ☒ Enable ☐ Disable

Parameters	Description
Access Control	Access Control allows you to specify which hosts users can or cannot have access to certain Internet applications
URL Blocking	URL Blocking allows you to specify which URLs can not be accessed by users.
DoS	The Broadband router's firewall can block common hacker attacks and can log the attack activities.
DMZ	The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN.

Click on one of the firewall selections and proceed to the manual's relevant sub-section

### 2.7.1 Access Control

If you want to restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.), this is the place to set that configuration. Access Control allows users to define the traffic type permitted in your LAN. You can control which PC client can have access to these services.

- System
- WAN
- LAN
- Wireless
- QoS
- NAT
- Firewall**
  - Access Control**
  - URL Blocking
  - DoS
  - DMZ
- Print Server
- File/FTP Server

### Security Settings (Firewall)

Access Control allows users to define the traffic type permitted or not permitted in your LAN. You can control which PC client uses what services in which they can have access to these services.  
If both of MAC filtering and IP filtering are enabled simultaneously, the MAC filtering table will be checked first and then IP filtering table.

☐ Enable MAC Filtering
 ☒ Deny
 ☐ Allow

Client PC MAC address	Comment
<input type="text"/>	<input type="text"/>

**MAC Filtering Table**

NO.	Client PC MAC address	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			

☐ Enable IP Filtering Table (up to 20 computers)
 ☒ Deny
 ☐ Allow

NO.	Client PC Description	Client PC IP address	Client Service	Protocol	Port Range	Select
<input type="button" value="Add PC"/> <input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>						

Parameters	Description
Deny	If select "Deny" then all PCs will be allowed to access Internet except for the PCs in the list below.
Allow	If select "Allow" then all PCs will be denied to access Internet except for the PCs in the list below.
Filter client PCs by IP	Fill "IP Filtering Table" to filter PC clients by IP.
Add PC	You can click Add PC to add an access control rule for users by IP addresses.
Remove PC	If you want to remove some PC from the "IP Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want remove all PCs from the table, just click "Delete All" button.
Filter client PC by MAC address	Check "Enable MAC Filtering" to enable MAC Filtering.
Add PC	Fill in "Client PC MAC Address" and "Comment" of the PC that is allowed to access the Internet, and then click "Add". If you find any typo before adding it and want to retype again, just click "Reset" and the fields will be cleared.
Remove PC	If you want to remove some PC from the "MAC Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want remove all PCs from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click "Reset".

You can now configure other advance sections or start using the router (with the advance settings in place)

### Access Control Add PC

This page allows users to define service limitation of client PC, including IP address and service type.

Client PC Description :

Client PC IP address :

 - 

Client PC Service :

Service Name	Detail Description	Select
WWW	HTTP, TCP Port 80, 3128, 8000, 8080, 8081	<input type="checkbox"/>
E-mail Sending	SMTP, TCP Port 25	<input type="checkbox"/>
News Forums	NNTP, TCP Port 119	<input type="checkbox"/>
E-mail Receiving	POP3, TCP Port 110	<input type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
MSN Messenger	TCP Port 1863	<input type="checkbox"/>
Telnet Service	TCP Port 23	<input type="checkbox"/>

AIM	AOL Instant Messenger, TCP Port 5190	<input type="checkbox"/>
NetMeeting	H.323, TCP Port 389,522,1503,1720,1731	<input type="checkbox"/>
DNS	UDP Port 53	<input type="checkbox"/>
SNMP	UDP Port 161, 162	<input type="checkbox"/>
VPN-PPTP	TCP Port 1723	<input type="checkbox"/>
VPN-L2TP	UDP Port 1701	<input type="checkbox"/>
TCP	All TCP Port	<input type="checkbox"/>
UDP	All UDP Port	<input type="checkbox"/>

**User Define Service**

**Protocol :** Both ▼

**Port Range :**

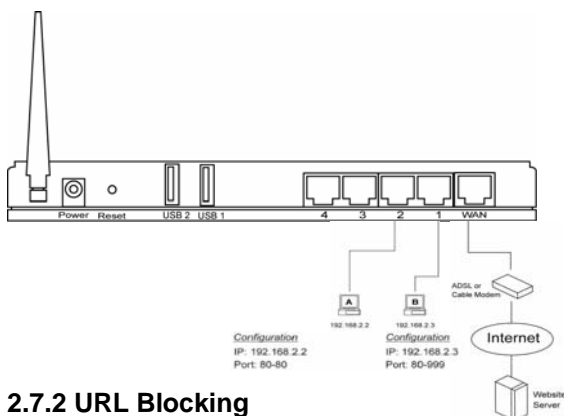
Add
Reset

Parameters	Description
Client PC Description	The description for this client PC rule.
Client PC IP Addresses	Enter the IP address range that you wish to apply this Access Control rule. This is the user's IP address (es) that you wish to setup an Access Control rule. <b>Note:</b> You need to give your LAN PC clients a fixed/static IP address for the Access Control rule to work properly.
Client PC Service	You can block the clients from accessing some Internet services by checking the services you want to block.
Protocol	This allows you to select UDP, TCP or both protocol types you want to block.
Port Range	It can be assign up to five port ranges. The router will block clients from accessing Internet services that use these ports.
Apply Changes	Click "Apply Changes" to save the setting.
Reset	Click "Reset" to clear all fields.

Click **<Apply Changes>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

#### Example: Access Control

In the example below, LAN client A can only access websites that use Port 80. However, LAN client B is able to access websites and any other service that uses ports between 80 and 999.



#### 2.7.2 URL Blocking

You can block access to some Web sites from particular PCs by entering a full URL address or just keyword of the Web site.

**EDIMAX**  
NETWORKING PEOPLE TOGETHER

Quick Setup
General Setup
Status Info
System Tools

- ☐ System
- ☐ WAN
- ☐ LAN
- ☐ Wireless
- ☐ QoS
- ☐ NAT
- ☒ Firewall
  - ☒ Access Control
  - ☒ URL Blocking
  - ☒ DoS
  - ☒ DMZ
- ☐ Print Server
- ☐ File/FTP Server

### URL Blocking

You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site.

☐ **Enable URL Blocking**

URL/Keyword

**Current URL Blocking Table**

NO.	URL/Keyword	Select
<div style="display: flex; justify-content: space-around; margin-top: 5px;"> <input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/> </div>		

Parameters	Description
Enable URL Blocking	Enable/disable URL Blocking
Add URL Keyword	Fill in "URL/Keyword" and then click "Add". You can enter the full URL address or the keyword of the web site you want to block. If you find any typo before adding it and want to retype again, just click "Reset" and the field will be cleared.
Remove URL Keyword	If you want to remove some URL keyword from the "Current URL Blocking Table", select the URL keyword you want to remove in the table and then click "Delete Selected". If you want remove all URL keyword from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click "Reset".

You can now configure other advance sections or start using the router (with the advance settings in place)

### 2.7.3 DoS (Denial of Service)

The Broadband router's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur the router can log the events.

**EDIMAX**  
NETWORKING PEOPLE TOGETHER

Quick Setup
General Setup
Status Info
System Tools

- ☐ System
- ☐ WAN
- ☐ LAN
- ☐ Wireless
- ☐ QoS
- ☐ NAT
- ☒ Firewall
  - ☒ Access Control
  - ☒ URL Blocking
  - ☒ DoS
  - ☒ DMZ
- ☐ Print Server
- ☐ File/FTP Server

### Denial of Service

The Broadband router's firewall can block common hacker attacks, including DoS, Discard Ping from WAN and Port Scan.

Denial of Service Feature	
Ping of Death	<input type="checkbox"/>
Discard Ping From WAN	<input type="checkbox"/>
Port Scan	<input type="checkbox"/>
Sync Flood	<input type="checkbox"/>

Parameters	Description
------------	-------------



Ping of Death	Protections from Ping of Death attack
Discard Ping From WAN	The router's WAN port will not respond to any Ping requests
Port Scan	Protection the router from Port Scan.
Sync Flood	Protection the router from Sync Flood attack.

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

#### 2.7.4 DMZ

If you have a local client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.

**Note:** The priority of FTP/HTTP server in DMZ is higher than that in NAS.

Parameters	Description
Enable DMZ	Enable/disable DMZ <b>Note:</b> If there is a conflict between the Virtual Server and the DMZ setting, then Virtual Server function will have priority over the DMZ function.
Public IP Address	The IP address of the WAN port or any other Public IP addresses given to you by your ISP
Client PC IP Address	Input the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address above <b>Note:</b> You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.

#### 2.8 Print Server

The router USB ports provide Print Server function to share printers for the network users. It supports LPD and IPP printing protocol.



**EDIMAX**  
NETWORKING PEOPLE TOGETHER

Quick Setup General Setup Status Info System Tools

System  
WAN  
LAN  
Wireless  
QoS  
NAT  
Firewall  
**Print Server**  
File/FTP Server

### Print Server

The printer server function supports LPR and IPP printing methods. You can enable/disable the print server function. Please assign the printer queue name to each printer connected USB port. It also supports Internet printing. Please refer to the manual for the detail information.

☐ **Enable Print Server**

**Print Server Protocol Support :**

IPP :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
LPR :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

**Print Server Configuration :**

Print Name of USB Port 1 :	<input type="text" value="lpt1"/>
Print Name of USB Port 2 :	<input type="text" value="lpt2"/>

☐ **Enable Internet printing**

Apply Cancel

Parameters	Description
Enable Print Server	Enable/disable USB print server. The print server function is disabled in default for better performance of NAS function.
IPP	Enable the Internet Printing Protocols.
LPR	Enable the Local Printing Remote Protocols.
Print Name of USB Port 1	Name of the printer connected to USB port 1.
Print Name of USB Port 2	Name of the printer connected to USB port 2.
Enable Internet printing	Enable Internet Printing to share the printer for Internet users.

Click **<Apply>** at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

### 2.8.1 LPR Printing

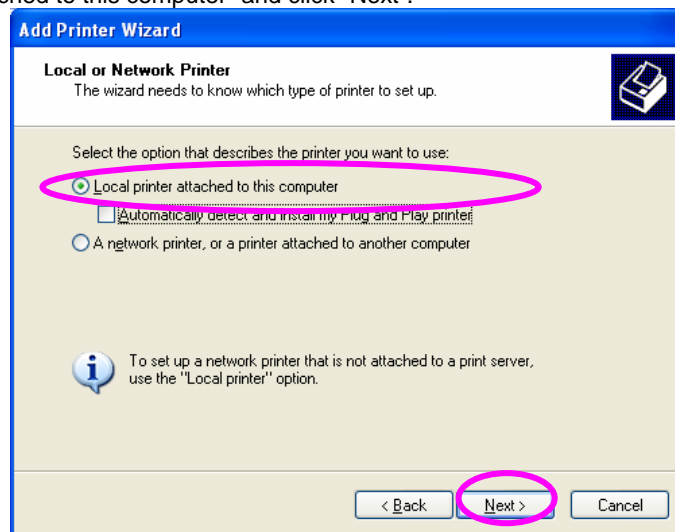
LPR Printing (Line Printer Remote technology) allows users to connect to printers via TCP/IP for printing sharing. The computer with Windows 98SE/Me/NT/2000/XP/2003 operating system can use the protocol to print documents in the network through Print Server.

To configure the LPR setting in Windows 2000/XP/2003, please follow the steps below.

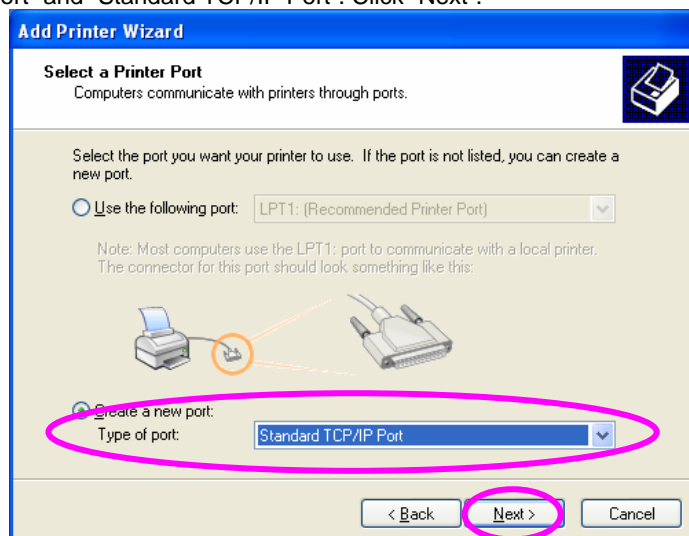
- 1) Click "Start", choose "Settings" and select "Printers and Faxes".
- 2) Click "Add a Printer".
- 3) When the "Add Printer Wizard" is displayed, click "Next".



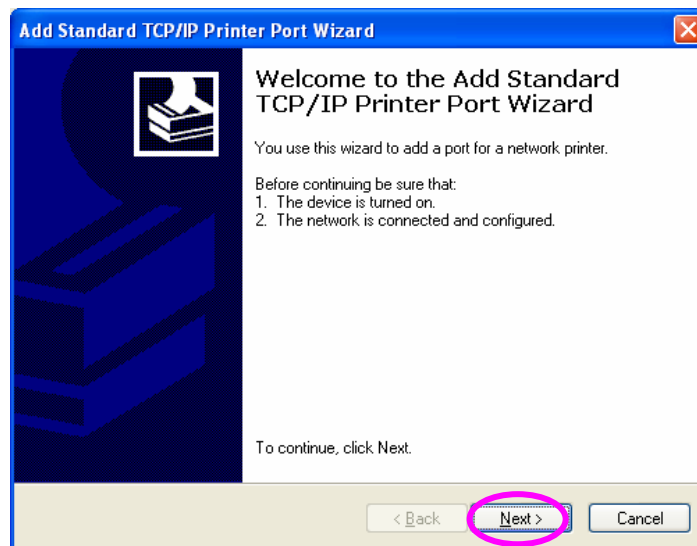
4) Select "Local Printer attached to this computer" and click "Next".



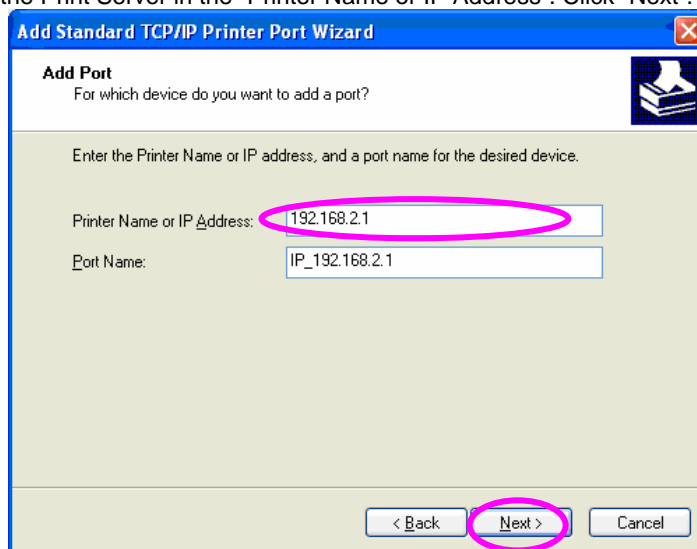
5) Choose "Create a new port" and "Standard TCP/IP Port". Click "Next".



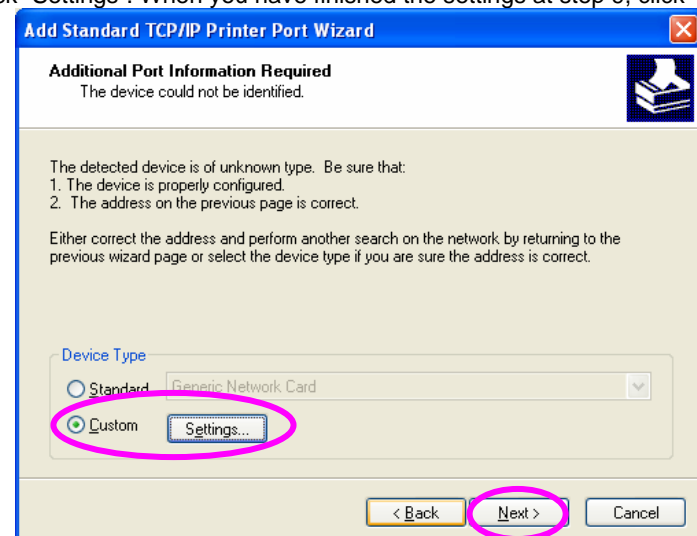
6) Please make sure that the Print Server and the Printer have turned on and connected to the network correctly before you continue. Click "Next".



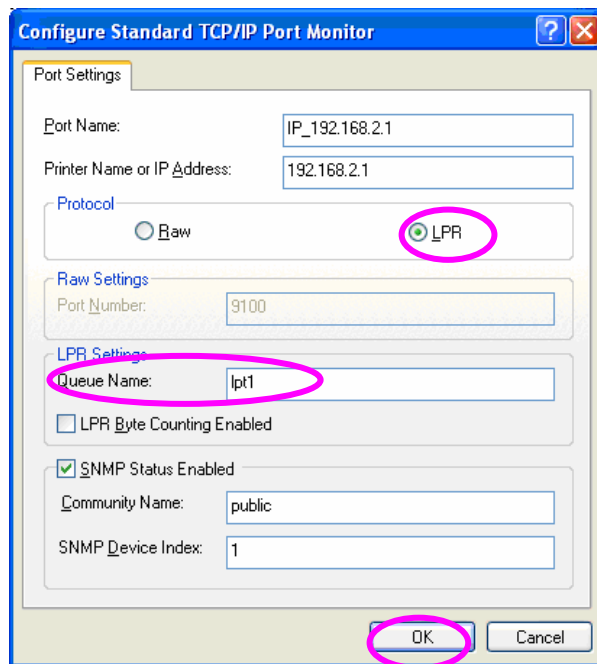
7) Enter the IP Address of the Print Server in the "Printer Name or IP Address". Click "Next".



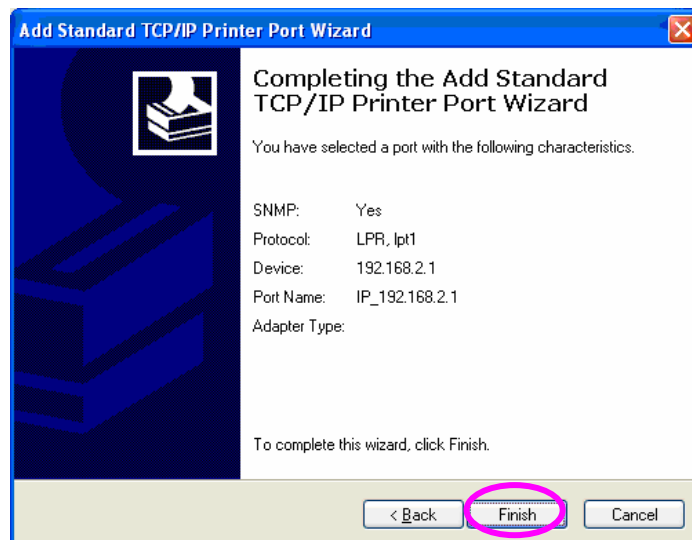
8) Select "Custom" and click "Settings". When you have finished the settings at step 9, click "Next" to continue.



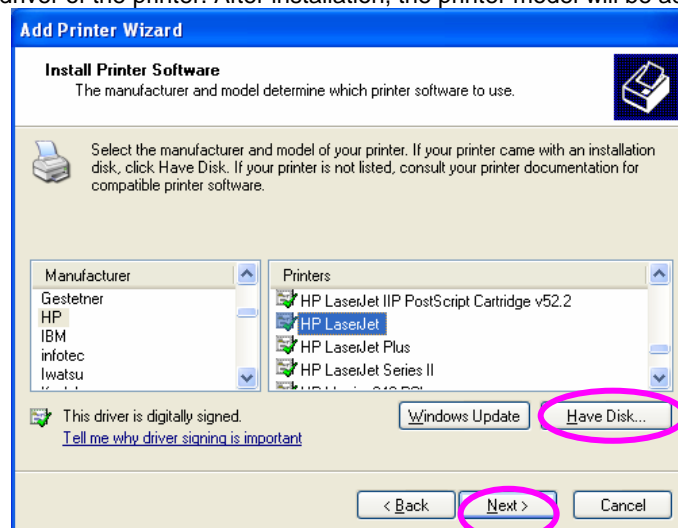
9) Select "LPR" and enter "lpt1" in the "Queue Name", click "OK". By default the queue name of the Print Server is "lpt1".



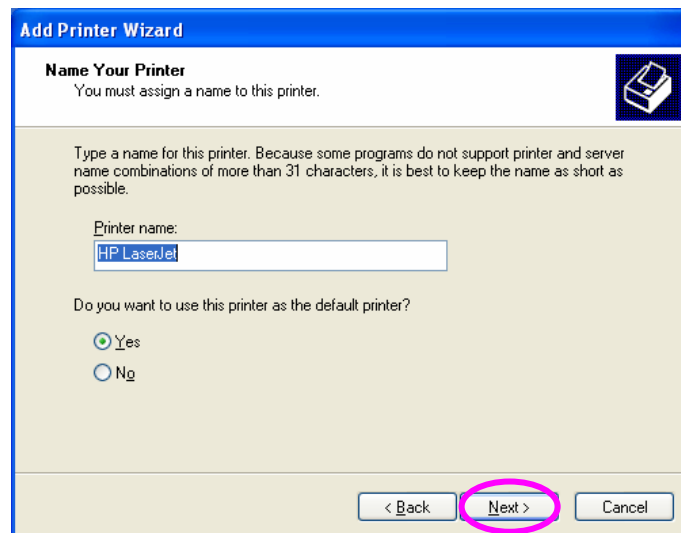
10) Click "Finish".



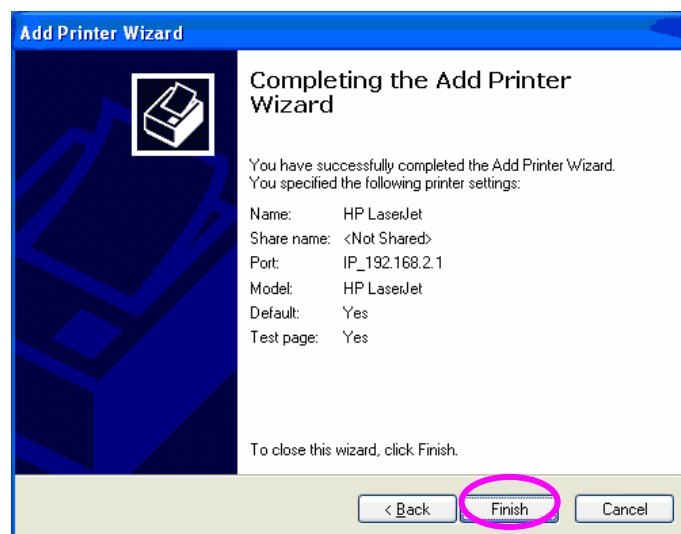
11) Select a suitable printer manufacturer and the printer model and click "Next". If your printer is not in the list, click "Have Disk..." to install the driver of the printer. After installation, the printer model will be added to the list.



12) Choose to set the print whether as a default printer or not. Click "Next".



13) You have added the network printer to the PC successfully. The information of the printer is displayed in the windows. Click "Finish".



## 2.8.2 IPP Printing

IPP (Internet Printing Protocol) Printing provides a convenient way of remote printing service by TCP/IP. The Print Server can support IPP printing in Windows 2000/XP/2003 by default. By using the IPP printing, you can share the printer to all the PC's that can access the Print Server by IP.

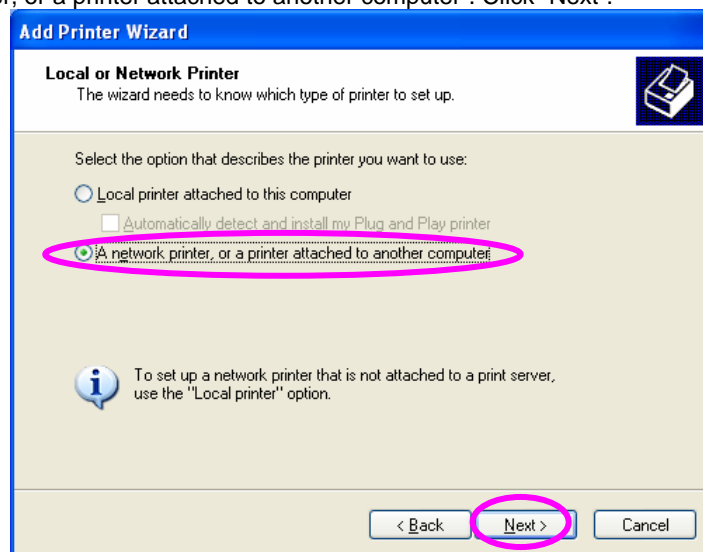
To configure the IPP Printing in Windows 2000/XP/2003, you have to make sure the Print Server has correct IP settings. If you want to share the printers to Internet users, you have to set a real IP to the Print Server. You also have to make sure that any gateway, router or firewall does not block IPP protocol if you have these gateway devices installed in your network.

At client side, please follow the steps below to configure the LPR setting in Windows 2000/XP/2003.

- 1) Click "Start", choose "Settings" and select "Printers and Faxes".
- 2) Click "Add a Printer".
- 3) The "Add Printer Wizard" is displayed. Click "Next".



4) Select "A network printer, or a printer attached to another computer". Click "Next".



5) Select "Connect to a printer on the Internet or on a home or office network" and enter the URL of Print Server. The URL format is "http://IP:631/Port Name". The IP should be the Print Server's IP. The number 631 is IPP standard port number. Port Name is the port name of Print Server that your printer is connected to. The default port name is "lpt1". One example of the URL is http://192.168.2.1:631/lpt1. After entering the URL of Print Server, click "Next".



**Add Printer Wizard**

**Specify a Printer**  
If you don't know the name or address of the printer, you can search for a printer that meets your needs.

What printer do you want to connect to?

☐ Browse for a printer

☐ Connect to this printer (or to browse for a printer, select this option and click Next):

Name:

Example: \\server\printer

☒ Connect to a printer on the Internet or on a home or office network:

URL:

Example: http://server/printers/myprinter/.printer

< Back   **Next >**   Cancel

6) Select a suitable printer manufacturer and the printer model and click "Next". If your printer is not in the list, click "Have Disk..." to install the driver of the printer. After installation, the printer model will be added to the list.

**Add Printer Wizard**

**Install Printer Software**  
The manufacturer and model determine which printer software to use.

Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.

Manufacturer:

Printers:

This driver is digitally signed. [Tell me why driver signing is important](#)

Windows Update   **Have Disk...**

< Back   **Next >**   Cancel

7) Choose to set the print whether as a default printer or not. Click "Next".

**Add Printer Wizard**

**Default Printer**  
Your computer will always send documents to the default printer unless you specify otherwise.

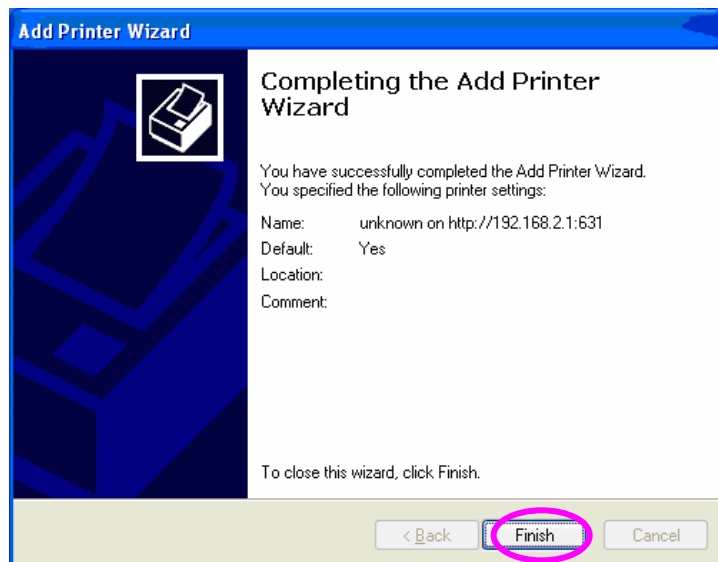
Do you want to use this printer as the default printer?

☒ Yes

☐ No

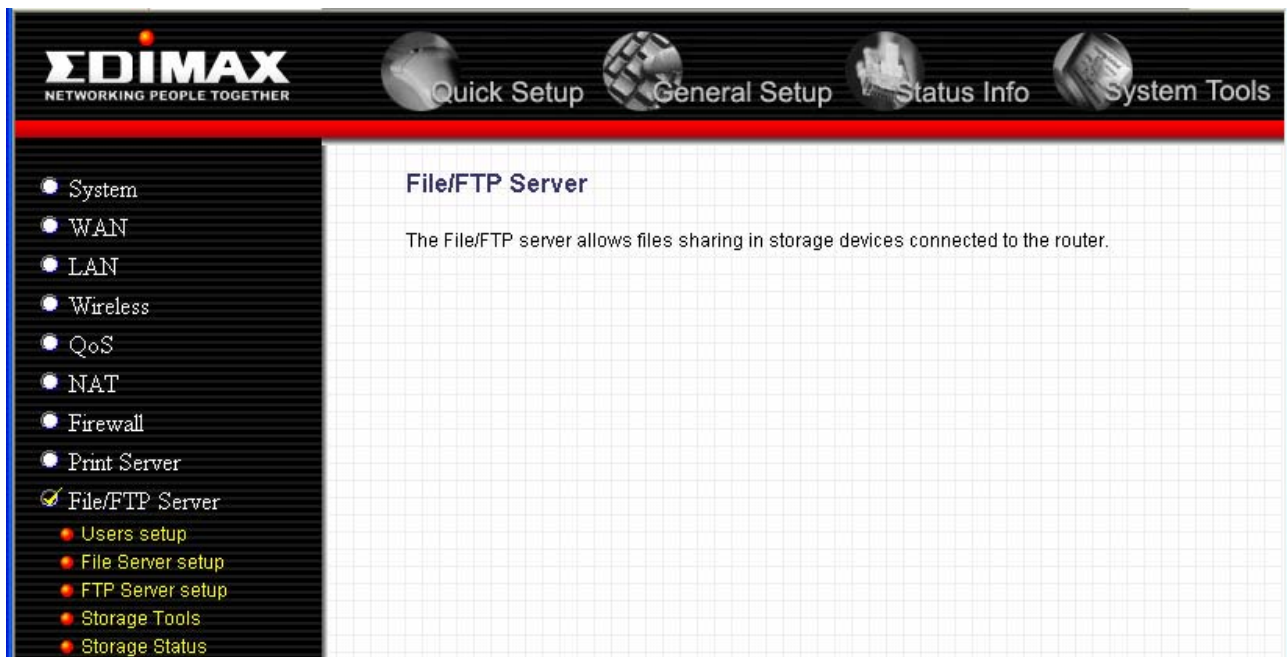
< Back   **Next >**   Cancel

8) You have added the network printer to the PC successfully. The information of the printer is displayed in the windows. Click "Finish".



## 2.9 File/FTP Server

The router provides File/FTP Server function to share USB storage devices to all PCs in Intranet/Internet. It supports SAMBA protocol in File Server so you can share files via My Network Places. It also supports FTP Server for FTP clients to upload/download files from the storage.



Parameters	Description
Users setup	Add/edit/delete users for File/FTP server accessing.
File Server setup	Add/edit the File Server name, shared folders and sharing policies via My Network Places.
FTP Server setup	Add/edit FTP folders and other advanced settings for FTP accessing.
Storage Tools	Manage the partitions of the USB storage devices. You can add, remove, or format the partition of the USB storage devices.
Storage Status	Show the status of both USB ports. When you plug a USB storage device into the USB port, it will show the status of the current valid disk and partition of this device.

Click on one of the File/FTP Server selections and proceed to the manual's relevant sub-section

**Note:** Due to operating system limitation, the maximum file size of a single file is less than 2GB in a partition of FAT16/32 file system. Whereas a partition of EXT2/3 file system, the file size is up to 4GB.

### 2.9.1 Users setup

Add/edit/delete users for File/FTP server.

**Users setup**

You can add/edit users for File/FTP server.

**Users list :**

User Name	Description	Select
thomas		<input type="checkbox"/>

Parameters	Description
Add	Click "Add" to fill the information of a new user for File/FTP server.
Edit	Select any user in Users list and click "Edit" to modify his profile.
Delete Selected	Click "Delete Selected" to delete the selected users in Users list.
Delete All	Click "Delete All" to delete all the users in Users list.
Reset	Click "Reset" to reset selection in Users list.

#### Add a New User

**Add a New User**

User Name :  (alphanumeric and underline)

Description :

Password :  (alphanumeric, space and underline)

Confirm password :  (alphanumeric, space and underline)

**ATTENTION:** User name and password are case sensitive, and the max length of these strings is 20.

Parameters	Description
------------	-------------

User Name	User name for this user.
Description	Description for this user.
Password	Password of this user.
Confirm password	Re-type the password of this user for confirmation.

Click **<Save>** at the bottom of the screen to save the settings. You can now configure other advanced sections or start using the router.

**NOTE:** The max length of these strings is 20.

### 2.9.2 File Server setup

You add/edit the File Server name, shared folders and sharing policies via My Network Places.

### File Server

**Storage name in the "My network places" :**

Name :  (alphanumeric and underline)

Workgroup :  (alphanumeric, space and underline)

Description :

You can add/edit shared folders below. All shared folders can be accessed from "My Network Places". Please assign the users' read/write authority for each shared folder. Attention: You cannot setup sharing policy here for folders in NTFS partitions.

**Shared Folders:**

Folder Name	Path	Description	Read	Write	Select
<div> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete All"/> <input type="button" value="Delete Selected"/> <input type="button" value="Reset"/> </div>					

The setting below will apply to any storage which you don't set any shared folder above. In this way, all users have the same authority ("Read & Write", "Read Only" or "Not to Share") to access folders in the storage. Attention: If the storage has NTFS partitions, all folders in NTFS partitions are "Read Only" even you choose "Read & Write" here.

**New Storage Default Sharing Policy**

☒ Read & Write  
☐ Read Only  
☐ Not to Share

Parameters	Description
Name	The File Server name in My Network Places.
Workgroup	The workgroup of this File Server in My Network Places
Description	A brief description for this File Server. This string will be shown in the detailed information of My Network Places.
Add	Click "Add" to fill the information of a new shared-folder for File server.
Edit	Select any shared folders in Shared Folders list and click "Edit" to modify its settings.
Delete All	Click "Delete All" to delete all the shared folders in Shared Folders list.
Delete Selected	Click "Delete Selected" to delete the selected shared folders in Shared Folders list.
Reset	Click "Reset" to reset selection in Shared Folders list.
Default Sharing Policy	Set a default sharing policy (Read & Write, Read Only or Not to Share) to any USB storage which you don't set any sharing policy.

### Add/Edit Shared Folder

The screenshot shows the EDIMAX web interface for configuring a shared folder. The sidebar on the left lists various system settings, with 'File/FTP Server' currently selected. The main content area is titled 'Add/Edit Shared Folder'. It includes the following fields and controls:

- Folder Name:** A text input field with a note '(alphanumeric and underline)'.
- Shared folder's Path:** A text input field with a 'Browse...' button next to it.
- Share all folders in storage:** A checkbox.
- Users:** A section with two lists: 'System Users' (containing 'thomas') and 'Share Users' (empty). Between the lists are buttons: 'Add >>', 'Add All >>', '<< Delete', and '<< Delete All'.
- Authority:** Radio buttons for 'Read Only' (selected) and 'Read & Write'.
- Description:** A text input field.
- Buttons:** 'Save', 'Reset', and 'Cancel' at the bottom.

Parameters	Description
Folder Name	The name for shared folder.
Shared Folder's Path	Click on "Browse" to select a sharing folder in the storage or click "Share all folders in storage" to share whole storage.
Users	Assign users to access this shared folder. Select the users from System Users and click "Add" to add into Share Users. You can also click "Add All" to add all users or remove the selected users from "Share Users".
Authority	Here you can assign the read/write authority for this shared folder. You can select "Read Only" for read only sharing or select "Read & Write" to give users full accessing right.
Description	Descriptions for this share folder.

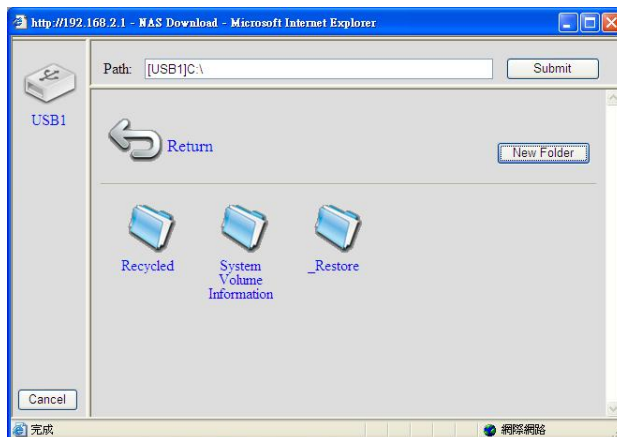
Click **<Save>** at the bottom of the screen to save the above settings. You can now configure other advanced sections or start using the router.



### Open Dialog

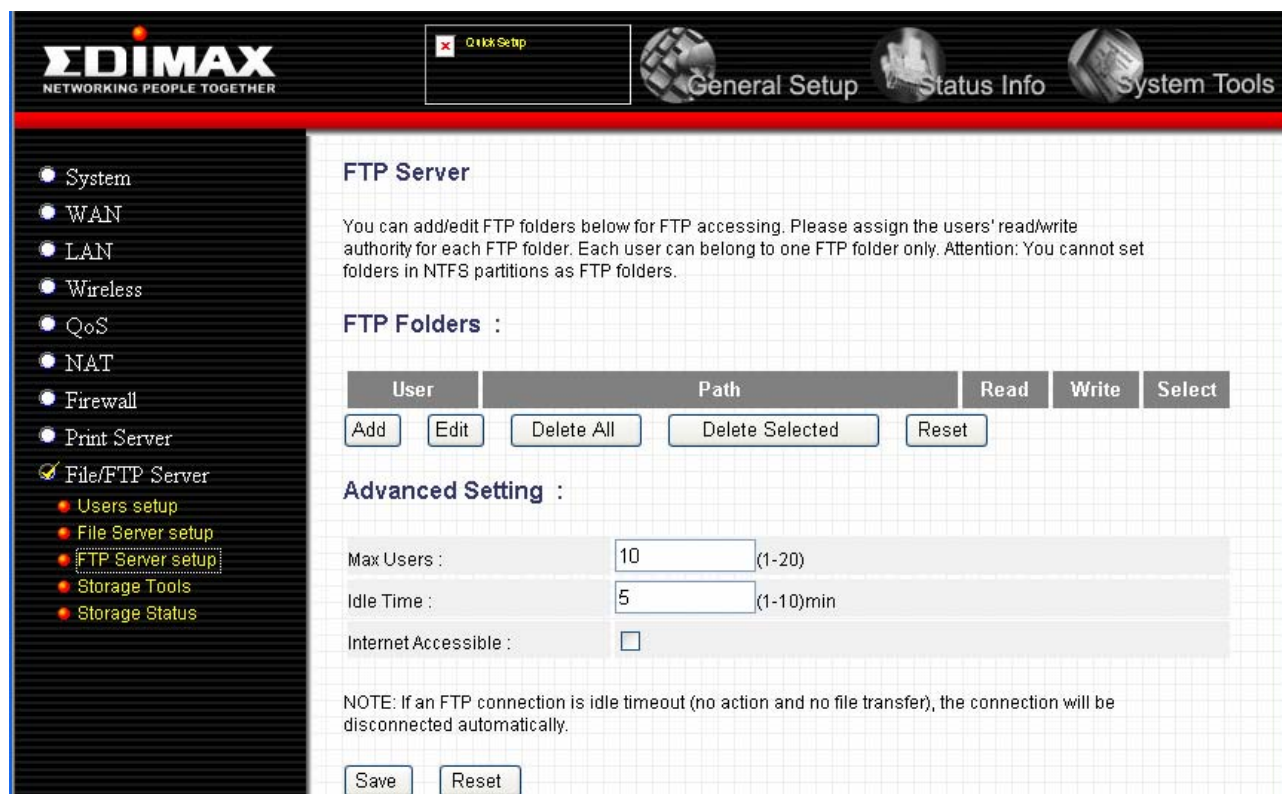
When you click the “Browse” button, you can see the following explorer window showing the USB storage devices. Please select the USB storage from left panel. The right panel will show the directories in this USB storage device. Choose the folder you want to share, and click “Submit” to select this folder. You can also click “New Folder” to create a new sharing folder.

**NOTE:** Only the folders in USB storage devices will be shown as icons in Open Dialog due to the sharing function is restricted to folders, not files.



### 2.9.3 FTP Server

You can add/edit/delete users, shared folders and sharing policies for sharing files via FTP service.



Parameters	Description
Add	Click “Add” to fill the information of a new shared-folder for FTP server.
Edit	Select any shared folders in FTP Folders list and click “Edit” to modify its settings.
Delete All	Click “Delete All” to delete all the shared folders in FTP Folders list.



Delete Selected	Click "Delete Selected" to delete the selected shared folders in FTP Folders list.
Reset	Click "Reset" to reset selection in FTP Folders list.
Max Users	Set the maximum concurrent users for the FTP server accessing.
Idle Time	Set the timeout period for FTP server to disconnect a FTP client when a FTP client is inactive longer than this time period..
Internet Accessible	Check this option to share FTP server in Internet or uncheck this option to use FTP server in Intranet.

#### Add/Edit FTP Folder

Parameters	Description
Users	Select the user for this FTP folder accessing.
Shared Folder's Path	Click on "Browse" to open the explorer window to select the sharing folder.
Authority	Assign the read/write authority for this FTP folder. You can select "Read Only" for read only sharing or select "Read & Write" to give users full accessing right.

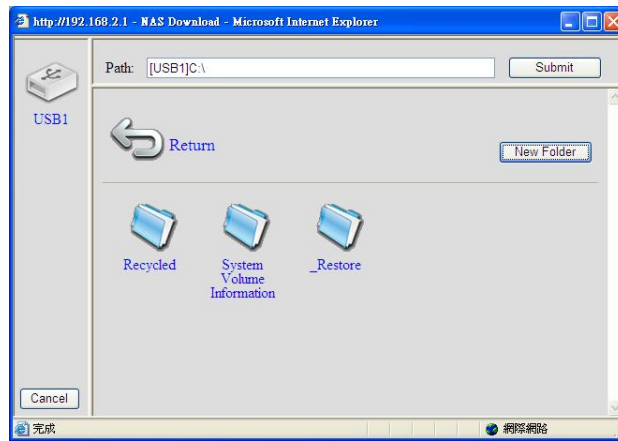
Click **<Save>** at the bottom of the screen to save the above settings. You can now configure other advanced sections or start using the router.

#### Open Dialog

When you click the "Browse" button, you can see the following explorer window that shows the USB storage devices. Please select the USB device from left panel. The right panel will show the directories in this USB storage device. Choose the folder you want to share, and click "Submit" to select this folder\.. You can also click "New Folder" to create a new FTP folder.

**NOTE:** Only the folders in USB storage devices will be shown as icons in Open Dialog due to the sharing function is restricted to folders, not files.

**NOTE:** Each user can only access to one FTP folder. Once a user is linked with one FTP folder, this user cannot access another FTP folder. But one FTP folder can be accessed by multi users.



## 2.9.4 Storage Tool

You can use the storage tools here to format, add or remove partitions.

**Note:** USB port 1 is usually for a brand new USB storage disk so you can use the Storage tools to partition and format the USB storage disk.

USB port 2 is for USB storage which you usually use to share data in other PC environment. If needed, you can partition and format in your favorite PC environment. You cannot partition or format the storage connected to USB port 2.

### Storage Tools

The table below shows all storage status. You can format, add partitions or remove. Before you apply any setting, please make sure that you are the only user in the setup page and the storage is always plugged and running during the whole progress. Otherwise, it may format this partition or remove other partition. This tool can only create or format a partition of the storage attached to USB Port 1. The Format tool cannot format the partition larger than 160GB. Also, the partition size should be larger than 32MB when you format the storage with FAT32.

**USB Port 1 :** Auto Partition & Format

Partition	Size	Start Cylinder	End Cylinder	File System	Tool	Select
free	99.6M	1	209	free	Format FAT32	<span style="border: 1px solid #4F81BD; padding: 2px 10px;">Add a Partition</span>
C	99.6M	210	418	FAT16	Format FAT32	<input type="checkbox"/>
D	59.6M	419	543	LINUX	Format FAT32	<input type="checkbox"/>
E	99.6M	544	752	FAT32	Format FAT16	<input type="checkbox"/>
					Format EXT2	<input type="checkbox"/>
free	125M	753	1014	free	Format FAT32	<span style="border: 1px solid #4F81BD; padding: 2px 10px;">Add a Partition</span>

Remove Selected Partitions
Remove All Partitions
Reset

Parameters	Description
Auto Partition & Format	Click this button to partition and format the USB storage disk in USB port 1 automatically.
Tool	Format the USB storage as FAT16, FAT32 or EXT2 system.
Add a Partition	Click this button to add a new partition in the USB storage.
Remove Selected Partitions	Click "Remove Selected Partitions" to remove the selected partitions in USB storage.
Remove All Partitions	Click "Remove All Partitions" to remove all the partitions in USB storage.
Reset	Click "Reset" to reset selection in the partition list.

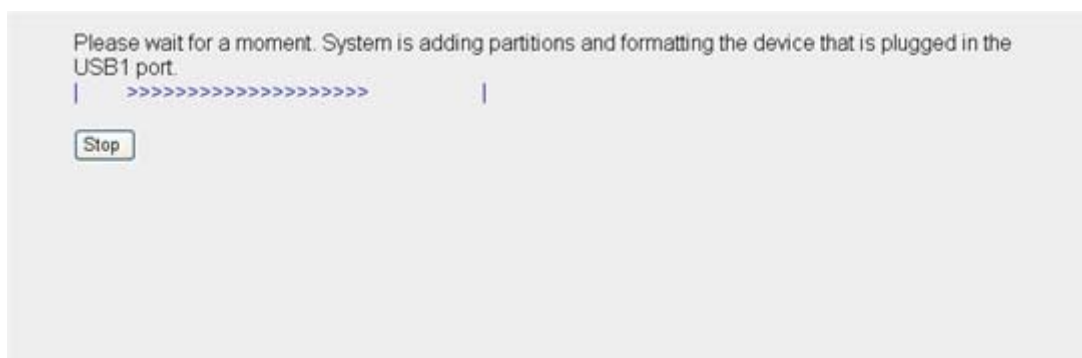
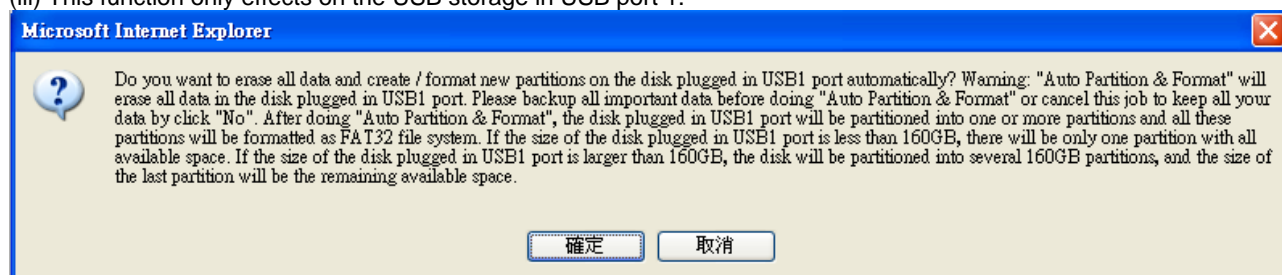
You can now configure other advanced sections or start using the router.

**NOTE:** The partition size with FAT16 file system should be less than 2GB. In FAT32 or EXT2 file system, the partition should be less than 160GB.

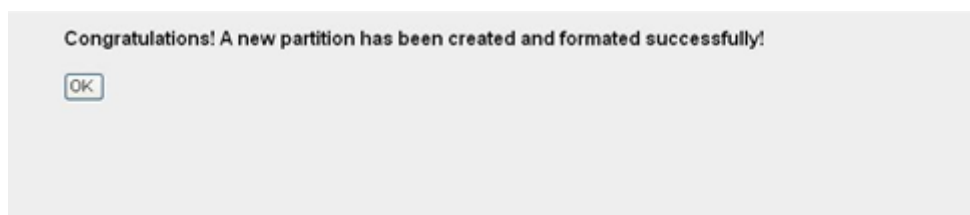
### Auto Partition & Formatting

This function is to partition and format the USB storage in USB port 1 according to the following rules.

- (i) It partitions the USB storage to 160GB each and formats to FAT32 file system.
- (ii) If the remaining size to partition is under 160GB, it will be partitioned as a partition.
- (iii) This function only effects on the USB storage in USB port 1.



**NOTE:** During partitioning, user can click the Stop button to stop the auto partition and back to Storage tools page to add or remove partition manually.



### Add Partition

This page is for you to add partition in the USB storage.

#### Add a Partition

You can create and format a new partition of the attached storage in this page.

Note: This tool can only create or format a partition of the storage attached to USB Port 1. The Format tool cannot format the partition larger than 160GB. Also, the partition size should be larger than 32MB when you format the storage with FAT32.

Size of the Space :	100MB
New Partition Size :	<input type="text" value="100"/> MB
File System :	<span>FAT32</span>

## 2.9.5 Storage Status

This Page shows the status of attached USB storages.

**EDIMAX**  
NETWORKING PEOPLE TOGETHER

Quick Setup General Setup Status Info System Tools

System  
WAN  
LAN  
Wireless  
QoS  
NAT  
Firewall  
Print Server  
File/FTP Server  
Users setup  
File Server setup  
FTP Server setup  
Storage Tools  
Storage Status

### Storage Status

This page shows the status of all valid partitions of attached storage. Any unformatted partition and any non-partitioned space of attached storage will not be displayed here.

USB Port 1 :

Partition	Size	Used	Free	Status
-----------	------	------	------	--------

USB Port 2 :

Partition	Size	Used	Free	Status
-----------	------	------	------	--------

Parameters	Description
Partition	The partition name in the USB storage.
Size	Total available space of this partition.
Used	Total used space of this partition. Here shows the byte count and the percentage of the total space.
Free	This shows free space of the specified partition.
Status	The partition type of the partition. It can be FAT16, FAT32, NTFS and Linux.
Unplug	You can click this button to unplug the USB storage disk.

You can now configure other advance sections or start using the router.

## Chapter 3

### Status

The Status section allows you to monitor the current status of your router. You can use the Status page to monitor: the connection status of the Broadband router's WAN/LAN interfaces, the current firmware and hardware version numbers, any illegal attempts to access your network, and information on all DHCP client PCs currently connected to your network.

System	
Model	Wireless Router
Up time	0day:1h:27m:30s
Hardware Version	Rev. A
Boot Code Version	1.0
Runtime Code Version	2.12

Parameters	Description
Status and Information	Shows the router's system information
Internet Connection	View the Broadband router's current Internet connection status and other related information
Device Status	View the Broadband router's current setting status
System Log	View the Broadband router's system log
Security Log	View any attempts that have been made to illegally gain access to your network.
Active DHCP Client	View your LAN client's information that is currently linked to the Broadband router's DHCP server
Statistics	Shows the statistics

Select one of the above Status selections and proceed to the manual's relevant sub-section

### 3.1 Status and Information

The Status and Information section allows you to view the router's system information

System	
Model	Wireless Router
Up time	0day:1h:27m:30s
Hardware Version	Rev. A
Boot Code Version	1.0
Runtime Code Version	2.12



Parameters	Description
Information	You can see the router's system information such as the router's: LAN MAC Address, WAN MAC Address, Hardware version, Serial Number, Boot code Version, Runtime code Version

### 3.2 Internet Connection

View the Broadband router's current Internet connection status and other related information

**Internet Connection**

View the current internet connection status and related information.

Attain IP Protocol :	Dynamic IP disconnect
IP address :	
Subnet Mask :	
Default Gateway :	0.0.0.0
MAC address :	00:5C:FC:62:15:64
Primary DNS :	
Secondary DNS :	

**Current Time**  
1/1/2000 1:34:11

Parameters	Description
Internet Connection	This page displays whether the WAN port is connected to a Cable/DSL connection. It also displays the router's WAN port: WAN IP address, Subnet Mask, and ISP Gateway as well as the Primary DNS and Secondary DNS being used.

### 3.3 Device Status

View the Broadband router's current configuration settings. The Device Status displays the configuration settings you've configured in the Quick Setup Wizard/General Setup section.

**Device Status**

View the current setting status of this device.

Wireless Configuration	
Mode	AP
Essid	default
Channel Number	11
Security	Disable

LAN Configuration	
IP address	192.168.2.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
MAC address	00:5c:fc:62:15:63

**Current Time**  
1/1/2000 1:34:45

Parameters	Description
------------	-------------



Device Status	This page shows the Broadband router's current device settings. This page displays the Broadband router LAN port's current LAN IP Address and Subnet Mask. It also shows whether the DHCP Server function is enabled/disabled.
---------------	--

### 3.4 System Log

View the operation log of the system.

The screenshot shows the EDIMAX web interface with the 'System Log' page selected. The left sidebar contains a 'Status' menu with options: Internet Connection, Device Status, System Log (highlighted), Security Log, Active DHCP Client, and Statistics. Below the menu is the 'Current Time' 1/1/2000 1:35:23. The main content area is titled 'System Log' and includes a description: 'View the system operation information. You can see the system start up time, connection process...etc. here.' Below this is a scrollable log window showing the following entries:

```
Jan 1 00:00:00 (none) syslog.info syslogd started: BusyBox v1.00-pre2 (200
Jan 1 00:00:12 (none) user.info udhcpd: udhcp server (v0.9.9-pre) started
Jan 1 00:00:15 (none) user.info udhcpd: udhcp client (v0.9.9-pre) started
Jan 1 00:00:29 (none) auth.info passwd[835]: password for `thomas' changed
Jan 1 00:00:30 (none) cron.notice crond[859]: ^Icrond 2.3.2 dillon, starte
Jan 1 00:13:36 (none) user.info udhcpd: sending OFFER of 192.168.2.100
Jan 1 00:13:36 (none) user.info udhcpd: sending ACK to 192.168.2.100
Jan 1 00:58:10 (none) user.info udhcpd: Received SIGTERM
Jan 1 00:58:22 (none) user.info udhcpd: udhcp server (v0.9.9-pre) started
```

At the bottom of the log window are three buttons: 'Save...', 'Clear', and 'Refresh'.

Parameters	Description
System Log	This page shows the current system log of the Broadband router. It displays any event occurred after system start up. At the bottom of the page, the system log can be saved <Save> to a local file for further processing or the system log can be cleared <Clear> or it can be refreshed <Refresh> to get the most updated situation. When the system is powered down, the system log will disappear if not saved to a local file.

### 3.5 Security Log

View any attempts that have been made to illegally gain access to your network.

The screenshot shows the EDIMAX web interface with the 'Security Log' page selected. The left sidebar contains a 'Status' menu with options: Internet Connection, Device Status, System Log, Security Log (highlighted), Active DHCP Client, and Statistics. Below the menu is the 'Current Time' 1/1/2000 1:36:07. The main content area is titled 'Security Log' and includes a description: 'View any attempts that have been made to illegally gain access to your network.' Below this is a scrollable log window showing the following entries:

```
[2000-01-01 00:00:14]: start Dynamic IP
[2000-01-01 00:32:35]: [SNTP]: connect to TimeServer 192.43.244.18 ...
[2000-01-01 00:32:35]: [SNTP]: connect fail!!
[2000-01-01 00:58:25]: start Dynamic IP
```

At the bottom of the log window are three buttons: 'Save...', 'Clear', and 'Refresh'.

Parameters	Description
Security Log	This page shows the current security log of the Broadband router. It displays any illegal attempts to access your network. At the bottom of the page, the security log can be saved <Save> to a local file for further processing or the security log can be cleared <Clear> or it can be refreshed <Refresh> to get the most updated situation. When the system is powered down, the security log will disappear if not saved to a local file.

### 3.6 Active DHCP Client

View your LAN client's information that is currently linked to the Broadband router's DHCP server

**Active DHCP Client**

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

IP address	MAC address	Time Expired(s)
None	----	----

Refresh

**Current Time**  
1/1/2000 1:36:48

Parameters	Description
Active DHCP Client	This page shows all DHCP clients (LAN PCs) currently connected to your network. The "Active DHCP Client Table" displays the <b>IP</b> address and the <b>MAC</b> address and Time Expired of each LAN Client. Use the <b>Refresh</b> button to get the most updated situation

### 3.7 Statistics

View the statistics of packets sent and received on WAN, LAN and Wireless LAN.

**Statistics**

This page shows the packet counters for transmission and reception regarding to networks.

Wireless LAN	Sent Packets	1666
	Received Packets	37006
Ethernet LAN	Sent Packets	13606
	Received Packets	27239
Ethernet WAN	Sent Packets	258
	Received Packets	0

Refresh

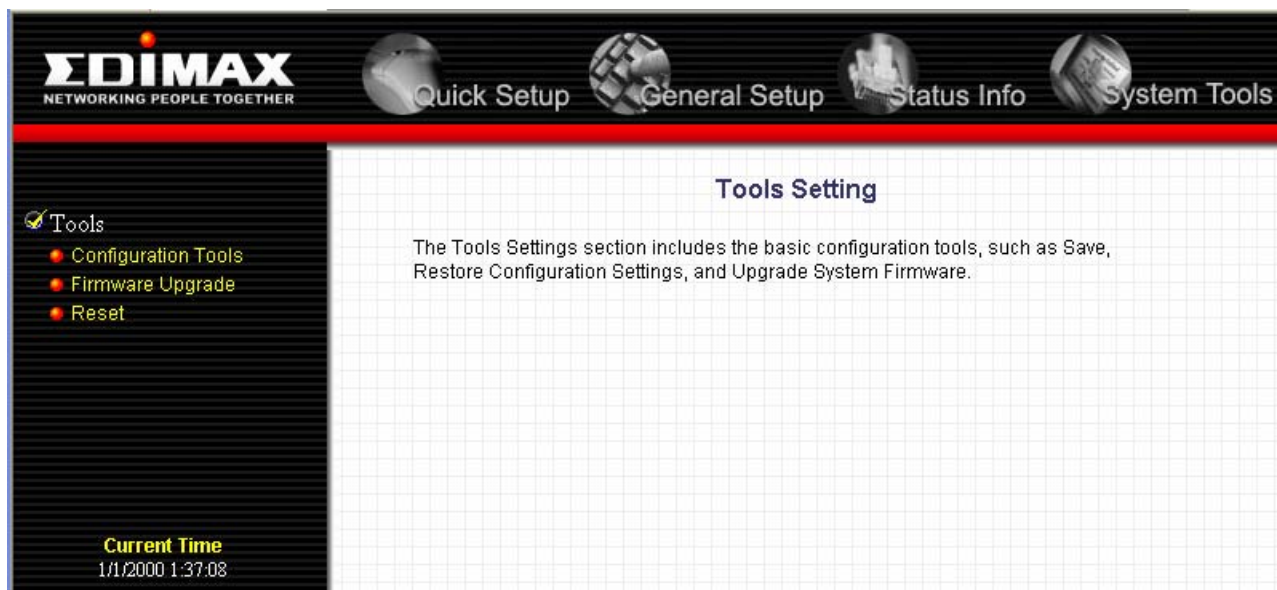
**Current Time**  
1/1/2000 1:37:39

Parameters	Description
Statistics	Shows the counters of packets sent and received on WAN, LAN and Wireless LAN.

## Chapter 4

### Tool

This page includes the basic configuration tools, such as Configuration Tools (save or restore configuration settings), Firmware Upgrade (upgrade system firmware) and Reset.

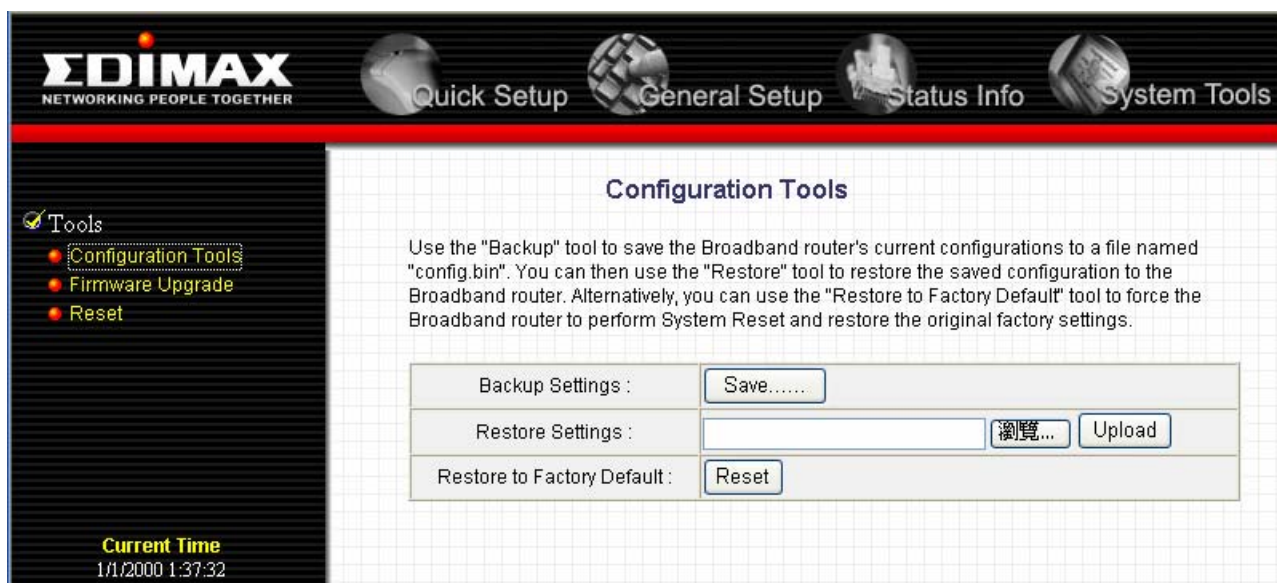


Parameters	Description
Configuration Tools	You can save the router's current configuration, restore the router's saved configuration files and restore the router's factory default settings
Firmware Upgrade	This page allows you to upgrade the router's firmware
Reset	You can reset the router's system should any problem exist

Select one of the above **Tools Settings** selection and proceed to the manual's relevant sub-section

### 4.1 Configuration Tools

The Configuration Tools screen allows you to save (**Backup**) the router's current configuration setting. Saving the configuration settings provides an added protection and convenience should problems occur with the router and you have to reset to factory default. When you save the configuration setting (Backup) you can re-load the saved configuration into the router through the **Restore** selection. If extreme problems occur you can use the **Restore to Factory Defaults** selection, this will set all configurations to its original default settings (e.g. when you first purchased the router).



Parameters	Description
------------	-------------

Configuration Tools	Use the " <b>Backup</b> " tool to save the Broadband router current configuration to a file named "config.bin" on your PC. You can then use the " <b>Restore</b> " tool to restore the saved configuration to the Broadband router. Alternatively, you can use the " <b>Restore to Factory Defaults</b> " tool to force the Broadband router to perform a power reset and restore the original factory settings.
---------------------	--



## 4.2 Firmware Upgrade

This page allows you to upgrade the router's firmware

**EDIMAX**  
NETWORKING PEOPLE TOGETHER

Quick Setup General Setup Status Info System Tools

**Firmware Upgrade**

This tool allows you to upgrade the Broadband router's system firmware. Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.

The system will automatically reboot the router after you finish the firmware upgrade process. If you don't complete the firmware upgrade process in the "next" step, you have to reboot the router.

Next

**Current Time**  
1/1/2000 1:38:04

Parameters	Description
Firmware Upgrade	If his tool allows you to upgrade the Broadband router's system firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.

Once you've selected the new firmware file, click **<Apply>** at the bottom of the screen to start the upgrade process. (You may have to wait a few minutes for the upgrade to complete). Once the upgrade is complete you can start using the router.

**Warning:** When upgrading firmware, be sure not to cut down the power or restart your computer.

## 4.3 Reset

You can reset the router's system should any problem exist. The reset function essentially re-boots your router's system

**EDIMAX**  
NETWORKING PEOPLE TOGETHER

Quick Setup General Setup Status Info System Tools

**Reset**

In the event that the system stops responding correctly or stops functioning, you can perform a Reset. Your settings will not be changed. To perform the reset, click on the APPLY button below. You will be asked to confirm your decision. The Reset will be complete when the LED Power light stops blinking.

Apply Cancel

**Current Time**  
1/1/2000 1:38:23

Parameters	Description
Reset	In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset. <b>Your settings will not be changed.</b> To perform the reset, click on the <b>&lt;APPLY&gt;</b> button. You will be asked to confirm your decision. The reset will be

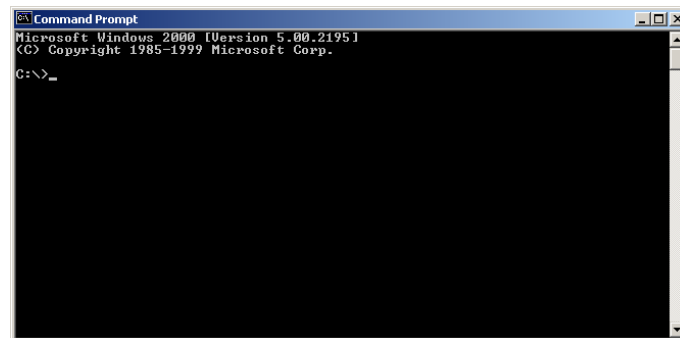


	complete when the power light stops blinking. Once the reset process is complete you may start using the router again.
--	--

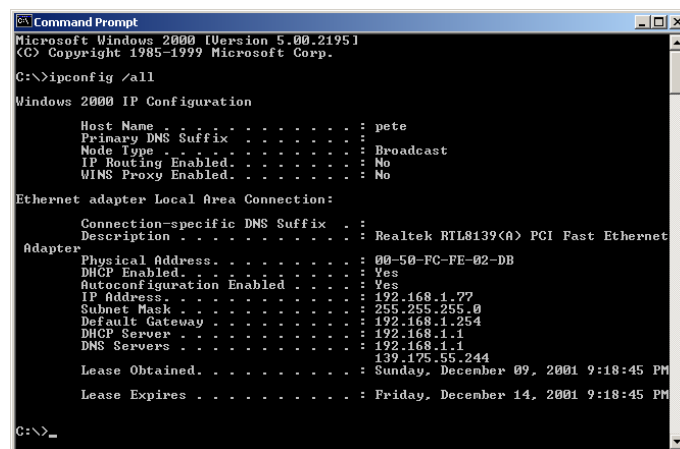
## Appendix A

### How to Manually find your PC's IP and MAC address

- 1) In Window's open the Command Prompt program



- 2) Type Ipconfig /all and <enter>



- Your PC's IP address is the one entitled **IP address** (192.168.1.77)
- The router's IP address is the one entitled **Default Gateway** (192.168.1.254)
- Your PC's MAC Address is the one entitled **Physical Address** (00-50-FC-FE-02-DB)

## Glossary

**Default Gateway (Router):** Every non-router IP device needs to configure a default gateway's IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out towards the destination.

**DHCP:** Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.

**DNS Server IP Address:** DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as [www.Broadbandrouter.com](http://www.Broadbandrouter.com)) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "Broadbandrouter.com" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

**DSL Modem:** DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

**Ethernet:** A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).

**Idle Timeout:** Idle Timeout is designed so that after there is no traffic to the Internet for a pre-configured amount of time, the connection will automatically be disconnected.

**IP Address and Network (Subnet) Mask:** IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, which identifies a single, unique Internet computer host in an IP network. Example: 192.168.2.1. It consists of 2 portions: the IP network address, and the host identifier.

The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by ".": aaa.aaa.aaa.aaa, where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers separated by ".": bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb, where each "b" can either be 0 or 1.

A network mask is also a 32-bit binary pattern, and consists of consecutive leading

1's followed by consecutive trailing 0's, such as

11111111.11111111.11111111.00000000. Therefore sometimes a network mask can also be described simply as "x" number of leading 1's.

When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1's in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form,

11011001.10110000.10010000.00000111, and if its network mask is,

11111111.11111111.11110000.00000000

It means the device's network address is

11011001.10110000.10010000.00000000, and its host ID is,

00000000.00000000.00000000.00000111. This is a convenient and efficient method for routers to route IP packets to their destination.

**ISP Gateway Address:** (see ISP for definition). The ISP Gateway Address is an IP address for the Internet router located at the ISP's office.

**ISP:** Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

**LAN:** Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered a LAN.

**MAC Address:** MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It is comprised of two parts: 3 bytes of data that corresponds to the Manufacturer ID (unique for each manufacturer), plus 3 bytes that are often used as the product's serial number.

**NAT:** Network Address Translation. This process allows all of the computers on your home network to use one IP address. Using the broadband router's NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

**Port:** Network Clients (LAN PC) uses port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

**PPPoE:** Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a secure data transmission method originally created for dial-up connections; PPPoE is for Ethernet connections. PPPoE relies on two widely accepted standards, Ethernet and the Point-to-Point Protocol. It is a communications protocol for transmitting information over Ethernet between different manufacturers

**Protocol:** A protocol is a set of rules for interaction agreed upon between multiple parties so that when they interface with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

**Router:** A router is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

**Subnet Mask:** A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

**TCP/IP, UDP:** Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocol. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

**WAN:** Wide Area Network. A network that connects computers located in geographically separate areas (e.g. different buildings, cities, countries). The Internet is a wide area network.

**Web-based management Graphical User Interface (GUI):** Many devices support a graphical user interface that is based on the web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to Control/configure or monitor the device being managed.

# **Federal Communication Commission**

## **Interference Statement**

### **FCC Part 68**

This equipment complies with Part 68 of the FCC Rules. On the bottom of this equipment is a label that contains the FCC Registration Number and Ringer Equivalence Number (REN) for this equipment. You must provide this information to the telephone company upon request.

The REN is useful to determine the quantity of devices you may connect to the telephone line and still have all of those devices ring when your number is called.

In most, but not all areas, the sum of the REN of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to your line, as determined by the REN, you should contact your local telephone company to determine the maximum REN for your calling area.

If the modem causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance.

But if advance notice isn't practical, you will be notified as soon as possible. You will be advised of your right to file a complaint with the FCC.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the proper operation of your equipment.

If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this modem, please contact your dealer for repair/warranty information. The telephone company may ask you to disconnect this equipment from the network until the problem has been corrected or you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

### **Installation**

This device is equipped with a USOC RJ11C connector.

### **FCC Part 15**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- 1.Reorient or relocate the receiving antenna.
- 2.Increase the separation between the equipment and receiver.
- 3.Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 4.Consult the dealer or an experienced radio technician for help.

**FCC Caution**

This equipment must be installed and operated in accordance with provided instructions and a minimum 20 cm spacing must be provided between computer mounted antenna and person's body (excluding extremities of hands, wrist and feet) during wireless modes of operation.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

**Federal Communication Commission (FCC) Radiation Exposure Statement**

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.



**R&TTE Compliance Statement**

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

**Safety**

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

**EU Countries Intended for Use**

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

**EU Countries Not intended for use**

None.

